Kapitel III.

Algebraische Gruppentheorie.

Von *Alfred Loewy* in Freiburg i. Br.

§ 1. Historisches. Definition der Gruppe. Beispiele. Das Feld oder der Körper.

Mag auch die Idee der Gruppe „implizit so alt wie der mathematische Gedanke sein“, so hat sich der Gruppenbegriff doch erst bei der Behandlung der algebraischen Gleichungen klar und deutlich herausgebildet. Lagrange wurde 1770 in seinen *Réflexions sur la résolution algébrique des équations, Œuvres* **3**, 205 (vgl. Pierpont, *Bull. Am. M. S.* **1**, 196 (1895)), Vandermonde in seiner *Résolution des équations* (1770) (deutsche Ausg., Berlin 1888) und vor allem Ruffini (vgl. Burkhardt, *Die Anfänge der Gruppentheorie und Paolo Ruffini, Ztschr. f. Math. u. Phys.* **37**, Suppl., S. 119 (1892) oder *Ann. di mat.* (2) **22**, 175 (1894)) bei seinen Unmöglichkeitsbeweisen für die algebraische Auflösbarkeit der Gleichungen von höherem als viertem Grad auf die Buchstabenvertauschungen oder die Lehre der *Permutationsgruppen* geführt. Cauchy (*J. éc. polyt.,* Cah. **17**, 1 u. 29 (1815), *Œuvres* (2) **1**, 64 u. 91, *Exercices d'analyse* **3** (1844), 151, *C. R.* **21** (1845), *Œuvres* (1) **9**, *C. R.* **22** (1846), *Œuvres* (1) **10**) hat die einzelnen Sätze seiner Vorgänger ergänzt, systematisch dargestellt und „in Terminologie und Bezeichnungsweise das Handwerkszeug geschaffen, dessen die Theorie der Permutationsgruppen zu ihrer Fortentwicklung benötigte“. Auch Abel (*Journ. f. Math.* **1**, 65 (1826), **4**, 131 (1829), *Œuvres par Sylow et Lie* (1881), **1**, 28, 66 u. 478, **2**, 217 u. 329) ist zu nennen; denn wie er stets gewöhnt war, „den höchsten Standpunkt einzunehmen“, so sind auch seine algebraischen Arbeiten von gruppentheoretischen Ideen durchtränkt.

Galois (1811—1832) (*Œuvres,* publ. par J. Liouville, *Journ. de math.* (1), **11**, 381 (1846), separat von Picard (1897)) verdankt man den für Gruppen im weitesten Sinn fundamentalen Begriff der *invarianten* Untergruppe sowie die hierauf gegründete Einteilung der Gruppen in *einfache* und *zusammengesetzte.* Von Galois stammt auch die Bezeichnung „Gruppe", Cauchy spricht von einem „système de substitutions conjuguées", eine Bezeichnung, die sich auch in J. A. Serrets *Algèbre supérieure* **2**, 3. éd., Paris 1866, findet. Die außerordentliche Bedeutung der Permutationsgruppen erhellt aus Galois' Nachweis, daß zu jeder algebraischen Gleichung eine Permutationsgruppe, die sogenannte Galoissche Gruppe, gehört; sie spiegelt alle Eigenschaften der betreffenden Gleichung wieder. C. Jordans *Traité des substitutions et des équations algébriques,* Paris 1870, bedeutet für die Theorie der Permutationsgruppen einen Markstein.

Die analytische Darstellung der Permutationsgruppen führte Galois (*Œuvres par Picard,* p. 27) auf eine auch unabhängig von den Buchstabenvertauschungen zu definierende Klasse endlicher Gruppen, die nach F. Klein (*Math. Ann.* **17**, 63 (1880)) sogenannten *Kongruenzgruppen.* Diese Schöpfung Galois', auf das innigste mit den sogenannten Galoisschen Imaginären oder dem Galoisschen Feld $GF[p^n]$ (vgl. unten) verknüpft, liefert uns eine ganze Reihe einfacher Gruppen. Unter den Gruppen endlicher Ordnungen sind die einfachen Gruppen die selteneren, aber auch die interessanteren; für eine große Anzahl algebraischer Gleichungen, welche der Funktionentheorie und Geometrie entspringen, sind sie von größter Wichtigkeit. Eine zusammenfassende Darstellung unserer Kenntnisse von den Kongruenzgruppen gibt das auch an eigenen Resultaten reiche Werk von L. E. Dickson, *Linear groups with an exposition of the Galois field theory, Teubners Samml.* **6**, Leipzig 1901. Neben ihm kommen für die älteren Untersuchungen in diesem Zweig der Gruppentheorie C. Jordans *Traité* sowie Klein-Fricke, *Theorie der elliptischen Modulfunktionen,* 2 Bde., Leipzig 1890/92, in Betracht.

Daß bei einer Gruppe nicht die Art der Darstellung der Elemente, sondern das Gesetz für ihre Kombination den springenden Punkt bildet, es sich also um Fragen eines allgemeineren und abstrakteren Gedankenkreises handelt, sprachen zuerst Cayley (1854) und (1878) (*Coll. math. papers* **2**, 123 und **10**, 401) und Kronecker (*Monatsb. d. Berl. Akad.* (1870), *Werke* **1**, 274) aus. Der Zweig der Gruppentheorie, der die

Gruppe unabhängig von der Darstellung ihrer Elemente studiert, wird als *abstrakte* oder *allgemeine Gruppentheorie* bezeichnet. Die Theorie der abstrakten Gruppen mit einer endlichen Anzahl von Elementen und die Theorie der Permutationsgruppen hängen auf das innigste durch den Satz zusammen: Jede endliche abstrakte Gruppe ist mit einer Permutationsgruppe holoedrisch isomorph, kann also durch eine Permutationsgruppe vertreten werden.

Der Begriff „Gruppe" ist aber nicht auf eine endliche Anzahl von Elementen beschränkt. Wäre man bei den linearen homogenen Differentialgleichungen genau auf die gleiche Weise vorgegangen wie Lagrange und Galois bei den algebraischen Gleichungen, so hätte man auf diesem Wege zu einem tieferen Studium der allgemeinen linearen homogenen Substitutionsgruppen und der Gruppen mit unendlich vielen Elementen gelangen können (vgl. E. Picard, *Traité d'analyse* **3**, Paris 1896, Chap. 16 u. 17, sowie die elementare Darstellung von A. Loewy, *Math. Ann.* **65**, 129 (1908)). Der historische Weg war ein anderer. Die Invariantentheorie der linearen homogenen Substitutionen oder, geometrisch gesprochen, die projektive Geometrie führte zu dem Begriff der Gruppe von unendlich vielen Elementen. Die Gruppe erscheint hier analytisch als die Gesamtheit der linearen homogenen Substitutionen:

$$x_i = a_{i1}x_1' + a_{i2}x_2' + \cdots + a_{in}x_n' \qquad (i = 1, 2, \ldots, n),$$

wobei die Determinante $|a_{ik}|$ $(i, k = 1, 2, \ldots, n)$ von Null verschieden ist. Deutet man die Variablen als homogene Punktkoordinaten eines $n-1$ dimensionalen Raumes, so hat man alle kollinearen Umformungen des R_{n-1}, d. h. alle Transformationen des R_{n-1}, die Punkte in Punkte überführen, vor sich. Die erste Arbeit, in der die unendliche Gruppe explizit eine wesentliche Rolle spielt, stammt von C. Jordan (*C. R.* **65**, 229 (1867), *Ann. di mat.* (2) **2**, 167 u. 322 (1869)). Bei Zugrundelegung rechtwinkliger Kartesischer Koordinaten findet eine Bewegung ihren analytischen Ausdruck in den Formeln:

$$\begin{aligned} x &= a_{11}x' + a_{12}y' + a_{13}z' + b_1, \\ y &= a_{21}x' + a_{22}y' + a_{23}z' + b_2, \\ z &= a_{31}x' + a_{32}y' + a_{33}z' + b_3, \end{aligned}$$

wobei die Matrix $\|a_{ik}\|$ $(i, k = 1, 2, 3)$ eine eigentliche orthogonale

Substitution (Kap. II, § 10) bestimmt. Die Gesamtheit aller angegebenen Operationen bildet die Bewegungsgruppe $\mathfrak{B}$. C. Jordans Problem ist das Studium aller Untergruppen der Bewegungsgruppe $\mathfrak{B}$.

Dann haben sich F. Klein und S. Lie des Gruppenbegriffes bemächtigt und vornehmlich ihnen ist es zu danken, daß sich die Gruppentheorie in fast allen Teilen der höheren Mathematik mehr und mehr Geltung verschaffte. S. Lie ist der Schöpfer der Theorie der kontinuierlichen Transformationsgruppen, die in einem besonderen Kapitel behandelt wird. Kleins sogenanntes Erlanger Programm (1872) *„Vergleichende Betrachtungen über neuere geometrische Forschungen“* (wiederabgedruckt: *Math. Ann.* **43**, 63 (1893)) will die ganze Geometrie als gruppentheoretisches Problem auffassen. Als weitere Ausführung dieser Ideen ist die autograph. Vorlesung *„Einleitung in die höhere Geometrie“* (Göttingen 1892/93) anzusehen. Vgl. auch Heffter und Köhler, *Lehrbuch der analytischen Geometrie*, Leipzig 1905. Bei Zugrundelegung rechtwinkliger Kartesischer Koordinaten erscheint die elementare Geometrie als das Studium aller Transformationen:

$$x = \lambda(a_{11}x' + a_{12}y' + a_{13}z') + b_1,$$
$$y = \lambda(a_{21}x' + a_{22}y' + a_{23}z') + b_2,$$
$$z = \lambda(a_{31}x' + a_{32}y' + a_{33}z') + b_3,$$

wobei die Matrix $\|a_{ik}\|$ $(i, k = 1, 2, 3)$ eine eigentliche orthogonale Substitution bestimmt. Der Inbegriff aller dieser Transformationen hat Gruppencharakter, er setzt sich aus Bewegungen, die man erhält, wenn die willkürliche Konstante $\lambda = 1$ gewählt wird, Ähnlichkeitstransformationen, Spiegelungen sowie allen hieraus resultierenden Transformationen zusammen. Diese Gruppe heißt nach F. Klein die *Hauptgruppe*. Man vgl. für diese Fragen besonders den Artikel von Fano, *Kontinuierliche geometrische Gruppen. Die Gruppentheorie als geometrisches Einteilungsprinzip, Encykl. d. math. Wiss.* **3**, S. 289. Vorzüglich beschäftigte sich F. Klein aber mit dem Studium der diskontinuierlichen endlichen wie unendlichen Gruppen, die er für eine Fülle der verschiedenartigsten Untersuchungen geometrischer, zahlentheoretischer und funktionentheoretischer Art verwendete. Seine Untersuchungen sind in folgenden Lehrbüchern zusammengefaßt: *Vorlesungen über das Ikosaëder und die Auflösung der Gleichungen vom 5. Grade* (Leipzig 1884). *Vorlesungen über die*

Theorie der elliptischen Modulfunktionen, herausg. von Fricke, 2 Bde., Leipzig 1890/92. Fricke u. Klein, *Vorlesungen über automorphe Funktionen*, Bd. 1, Leipzig 1897, Bd. 2, 1. Lieferung 1901.

Außer den schon zitierten Werken kommen für die in diesem Kapitel zu behandelnden Gegenstände hauptsächlich folgende Lehrbücher in Frage:

Für das Gesamtgebiet: H. Weber, *Lehrbuch der Algebra*. Bd. 1 u. 2, Braunschweig, 2. Aufl. 1898 u. 1899.

Für Permutationsgruppen: E. Netto, *Substitutionentheorie und ihre Anwendungen auf Algebra*, Leipzig 1882.

Bianchi, *Lezioni sulla teoria dei gruppi di sostituzioni*, Pisa 1900.

Für abstrakte Gruppen: J. A. de Séguier, *Éléments de la théorie des groupes abstraits*, Paris 1904.

Für endliche abstrakte Gruppen und Permutationsgruppen: W. Burnside, *Theory of groups of finite order*, Cambridge 1897, E. Netto, *Gruppen- und Substitutionentheorie, Samml. Schubert* **55**, Leipzig 1908.

Eine eingehende Zusammenstellung der Literatur und der Lehrsätze über Permutationsgruppen und endliche abstrakte Gruppen gibt B. S. Easton, *The constructive development of group-theory with a bibliography*, Boston 1902. Sehr schätzenswerte Führer in der neueren gruppentheoretischen Literatur sind die Referate von G. A. Miller, *Bull. Am. M. S.* (2) **5**, 227—249 (1899), (2) **9**, 106—123 (1902), (2) **14**, 78—91, 124—133 (1907), (2) **7**, 121—130 (1900), sowie von L. E. Dickson, ebenda (2) **6**, 13—27 (1899). Schließlich sei noch auf die Artikel „*Endliche diskrete Gruppen*“ von H. Burkhardt und „*Endliche Gruppen linearer Substitutionen*“ von A. Wiman in der *Encyklopädie der math. Wiss.* **1**, 208 u. 522 verwiesen.

Eine *Gruppe* läßt sich auf folgende Weise *definieren:* Für ein System 𝔊 von Elementen — man sagt auch Dingen, Operatoren — A, B, C, ... sei irgendeine Vorschrift gegeben, die aus zwei beliebigen gleichen oder ungleichen Elementen A und B eindeutig stets ein drittes C bestimmt. Man schreibt $C = AB$. Das Verfahren wird als Komposition oder Multiplikation bezeichnet, C heißt das Produkt von A und B oder auch das Resultat der Komposition von A und B.

Die Elemente von 𝔊 bilden eine Gruppe, wenn sie, außer

daß sie untereinander komponiert werden können, noch die folgenden vier Postulate erfüllen:

1. Das Produkt irgend zweier Elemente von 𝔊 gehört 𝔊 an.

2. Die Produktbildung ist assoziativ, d. h. sind A, B, C irgend drei Elemente aus 𝔊, so soll $A(BC) = (AB)C$ sein.

3. In 𝔊 gibt es wenigstens ein Element J, so daß für jedes Element A von 𝔊 die Gleichung $AJ = A$ gilt. (J heißt rechtshändiges Einheitselement.)

4. Existieren Elemente J, so soll für ein besonderes J und für jedes A die Gleichung $AX = J$ durch ein Element von 𝔊 lösbar sein.

Die angegebenen vier Postulate sind *voneinander unabhängig,* d. h. es läßt sich aus drei von ihnen niemals das vierte als beweisbarer Lehrsatz ableiten. Die vier Postulate bleiben auch voneinander unabhängig, wenn man zu ihnen noch ein fünftes über die Anzahl der verschiedenen Elemente von 𝔊 hinzufügt: Die Anzahl der verschiedenen Elemente von 𝔊

5_1) sei gleich n, wobei n eine beliebige endliche Zahl ist, oder

5_2) sie bestehe aus einer abzählbar unendlichen Menge oder

5_3) sie bilde eine nicht abzählbare unendliche Menge.

Die gegebene Definition einer abstrakten Gruppe durch voneinander unabhängige Postulate ist die Moore-Dicksonsche (E. H. Moore, *Trans. Am. M. S.* **3**, 485 (1902), **5**, 549 (1904), **6**, 179, L. E. Dickson, ebenda **6**, 198 (1905)). Wegen anders gefaßter Definitionen einer abstrakten Gruppe vgl. Huntington, *Trans. Am. M. S.* **6**, 181 (1905).

Man beweist: *Eine auf die obige Weise definierte Gruppe 𝔊 enthält nur ein einziges Einheitselement;* es läßt sowohl als linkshändiger oder vorderer Faktor wie als rechtshändiger oder hinterer Faktor jedes Element von 𝔊 ungeändert. *Dieses einzige Einheitselement wird im folgenden ausnahmslos mit **E** oder* 1 *bezeichnet.*

Auf Grund der eingeführten Postulate beweist man ferner: Zu jedem Element A von 𝔊 gibt es in 𝔊 ein und auch nur ein Element X, das gleichzeitig den zwei Gleichungen $AX = E$ und $XA = E$ genügt. Dieses Element X wird mit A^{-1} bezeichnet und heißt das zu A *inverse* oder *reziproke* Element. Es ist also $AA^{-1} = A^{-1}A = E$.

Für das reziproke Element eines Produktes AB gilt die Relation

$$(AB)^{-1} = B^{-1}A^{-1}.$$

Setzt man ein Element A α-mal als Faktor, so wird das Resultat der Komposition mit A^α bezeichnet und die *α^{te} Potenz von A* genannt. Unter A^0 soll das Einheitselement E verstanden werden. Setzt man A^{-1} α-mal als Faktor, so entsteht ein Element, das mit $A^{-\alpha}$ bezeichnet wird. $(A^{-1})^\alpha = A^{-\alpha}$ ist das reziproke Element von A^α. Für positive und negative ganzzahlige Werte von α und β gilt ebenso wie für verschwindende α und β die Relation

$$A^\alpha A^\beta = A^\beta A^\alpha = A^{\alpha+\beta}.$$

Eine Gruppe $\mathfrak{G}$ mit einer endlichen Anzahl verschiedener Elemente heißt eine *endliche Gruppe.* Besitzt die endliche Gruppe $\mathfrak{G}$ n verschiedene Elemente, so heißt n die *Ordnung der Gruppe* (Cauchy bedient sich schon der Bezeichnung „ordre", H. Weber, *Algebra* **2**, 4 verwendet abweichend vom üblichen Sprachgebrauch Grad für Ordnung), und man *schreibt* $\mathfrak{G}_n$. Eine Gruppe mit unendlich vielen Elementen heißt eine *unendliche Gruppe.*

Bei einer Gruppe ist das Produkt AB zweier Elemente im allgemeinen von dem Produkt BA verschieden. Ist das Produkt zweier Gruppenelemente A und B unabhängig von der Reihenfolge der Faktoren, ist also $AB = BA$, so heißen die Elemente A und B *vertauschbar* oder *kommutativ.* Jedes Gruppenelement ist mit seinen positiven wie negativen Potenzen vertauschbar. Das Einheitselement ist mit allen Gruppenelementen vertauschbar.

Eine Gruppe, die nur aus vertauschbaren Elementen besteht, heißt eine *vertauschbare, kommutative* oder *Abelsche* Gruppe. Der letztere Name ist mit Rücksicht auf die Eigenschaften der von Abel untersuchten besonderen Klasse algebraisch auflösbarer Gleichungen gegeben worden, die eine vertauschbare Galoissche Gruppe haben (Abel, *Mémoire sur une classe particulière d'équations résolubles algébriquement, Journ. f. Math.* **4**, 131 (1829), *Œuvres par Sylow et Lie* **1**, 478, deutsche Ausgabe mit Anm. von A. Loewy in *Ostwalds Klassikern der exakten Wiss.* No. 111).

Eine Gruppe, die nur aus den Potenzen eines einzigen Elementes besteht, also bloß die Elemente:

$$\ldots, A^{-2}, A^{-1}, A^0, A, A^2, \ldots$$

umfaßt, heißt *zyklisch.* Es gibt sowohl endliche als auch un-

endliche zyklische Gruppen. Jede zyklische Gruppe ist eine kommutative Gruppe.

Ein Beispiel für eine nicht kommutative unendliche Gruppe gibt die Gesamtheit aller Matrices gleichen Grades von nichtverschwindenden Determinanten, wenn man sie komponiert; Einheitselement der Gruppe ist hierbei die Einheitsmatrix (vgl. Kap. II, § 6). Weitere Beispiele nichtkommutativer unendlicher Gruppen sind: die Gesamtheit aller Matrices gleichen Grades, deren Determinanten den absoluten Betrag 1 haben, die Gesamtheit aller Matrices gleichen Grades, deren Determinanten den Wert ± 1 haben, die Gesamtheit aller Matrices gleichen Grades, die orthogonale Substitutionen bestimmen, die Gesamtheit aller Matrices, deren Koeffizienten rationale Zahlen oder algebraische Zahlen sind, falls man sie nach dem für Matrices geltenden Kalkül komponiert. Einheitselement bei diesen Gruppen ist stets die Einheitsmatrix.

Durch jedes System höherer komplexer Zahlen werden Gruppen bestimmt (vgl. S. 99ff.).

Als geometrisches Beispiel für eine unendliche nichtkommutative Gruppe kann die schon oben erwähnte Gesamtheit aller kollinearen Umformungen des Raumes dienen. Jede Raumtransformation, die Punkte in Punkte überführt, ist eine eindeutig umkehrbare Operation. Werden zwei solche Transformationen nacheinander ausgeführt, so läßt sich ihr Resultat stets durch eine dritte derselben Art erzielen. Für die Zusammensetzung von Kollineationen gilt offenbar auch das assoziative Gesetz. Die Gesamtheit der kollinearen Umformungen des Raumes hat also Gruppencharakter; man bezeichnet diese Gruppe auch als *„allgemeine projektive Gruppe“*. Die allgemeine Form einer einzelnen projektiven Transformation lautet für unseren R_3 in unhomogenen Punktkoordinaten x, y, z:

$$x = \frac{a_{11}x' + a_{12}y' + a_{13}z' + a_{14}}{a_{41}x' + a_{42}y' + a_{43}z' + a_{44}},$$

$$y = \frac{a_{21}x' + a_{22}y' + a_{23}z' + a_{24}}{a_{41}x' + a_{42}y' + a_{43}z' + a_{44}},$$

$$z = \frac{a_{31}x' + a_{32}y' + a_{33}z' + a_{34}}{a_{41}x' + a_{42}y' + a_{43}z' + a_{44}},$$

wobei die Konstanten a_{ik} nur der Bedingung zu genügen haben, daß die Determinante $|a_{ik}|$ $(i, k = 1, 2, 3, 4)$ nicht verschwinden darf.

Die allgemeine projektive Gruppe umfaßt die Hauptgruppe wie die Bewegungsgruppe (vgl. oben S. 171).

Beispiele für endliche, nichtkommutative Gruppen werden im folgenden in der Form von Permutationsgruppen, Kongruenzgruppen und endlichen Gruppen linearer homogener Substitutionen behandelt werden. Wir begnügen uns damit, an dieser Stelle auf ein durch die Geometrie geliefertes Beispiel hinzuweisen, nämlich auf gewisse in der Bewegungsgruppe unseres Raumes enthaltene Gruppen, die endlichen Gruppen der regulären Körper. Die Gesamtheit der Drehungen, die einen regulären Körper mit sich selbst zur Deckung bringen, bildet eine Gruppe. Das Tetraëder wird durch 12, das Oktaëder und der Würfel durch 24, das Ikosaëder und das Dodekaëder durch 60 Drehungen mit sich selbst zur Deckung gebracht.

Eine unendliche kommutative Gruppe bildet beispielsweise die Gesamtheit unserer gemeinen komplexen Zahlen $a + ib$, wenn man die gewöhnliche Addition als Komposition der Elemente ansieht. Einheitselement dieser Gruppe ist die Null. Eine unendliche kommutative Gruppe wird auch bei Ausschluß der Null von der Gesamtheit unserer gemeinen komplexen Zahlen $a + ib$ gebildet, wenn man die gewöhnliche Multiplikation als Komposition der Elemente auffaßt. Einheitselement der Gruppe ist hierbei die Zahl 1.

Die bei dem System der gemeinen komplexen Zahlen entgegentretende doppelte Verknüpfungsfähigkeit der Elemente mit Gruppencharakter führt zum Begriff des *Feldes* oder *Körpers* oder *Rationalitätsbereiches*. Wir betrachten ein System $\mathfrak{C}$ von Elementen, die sich auf zwei Arten verknüpfen lassen. In bezug auf die erste Verknüpfung, die als Addition bezeichnet wird, sollen die Elemente von $\mathfrak{C}$ eine Gruppe bilden. Für die zweite Art der Komposition, die Multiplikation heiße, wird verlangt, daß die Elemente von $\mathfrak{C}$, wenn man die Einheit der additiven Gruppe, die 0 heiße, ausschließt, eine kommutative Gruppe bilden. Die Multiplikation der Elemente von $\mathfrak{C}$ mit 0 soll nach der Relation $0 \cdot x = x \cdot 0 = 0$ statthaben. Schließlich soll die Multiplikation der Elemente von $\mathfrak{C}$ in Verbindung mit der Addition distributiv sein. $a(b + c) = ab + ac$. Genügen die Elemente von $\mathfrak{C}$ den angeführten Bedingungen, so ist, wie man beweisen kann, auch die bei der additiven Verknüpfung der Elemente von $\mathfrak{C}$ entstehende Gruppe kommutativ (vgl. Hilbert, *Math.-Ver.* 8, 183 (1899)). Ein System $\mathfrak{C}$, dessen Elemente den obigen Bedingungen genügen, heißt ein *Feld*, *Körper* oder

Rationalitätsbereich. Kurz kann das Feld als ein in sich abgeschlossenes Elementensystem definiert werden, für das die gewöhnlichen Sätze der Algebra gelten. Abstrakte Definitionen des Feldes geben H. Weber, *Math. Ann.* **43**, 526 (1893), Dickson, *Trans. Am. M. S.* **4**, 13 (1903), **6**, 198 (1905), Huntington, ebenda **4**, 31 (1903) und **6**, 181 (1905). Unendliche Felder sind: die rationalen Zahlen, alle reellen Zahlen, alle algebraischen Zahlen, die Gesamtheit aller Zahlen, wenn man sie in gewöhnlicher Weise additiv und multiplikativ verknüpft. Die abstrakten Definitionen für den Körper lassen sich auch zur Einführung der gemeinen komplexen Zahlen unseres Zahlensystems verwenden. Vgl. Huntington, *A set of postulates for real algebra, for ordinary complex algebra, Trans. Am. M. S.* **6**, 17 und **6**, 209 (1905).

Fundamental ist die Existenz *endlicher Felder* oder *endlicher Körper,* d. h. solcher mit nur endlich vielen verschiedenen Elementen.

Ist p eine positive Primzahl, so erhält man auf folgende Weise ein endliches Feld mit p verschiedenen Elementen: Wir teilen die ganzen positiven Zahlen mod p in p Klassen, so daß alle mod p kongruenten Zahlen derselben Klasse angehören, während mod p inkongruente Zahlen in verschiedene Klassen fallen:

$$\begin{array}{lllll} K_0: & 0, & p, & 2p, & 3p, \quad \dots \\ K_1: & 1, & p+1, & 2p+1, & 3p+1, \dots \\ K_2: & 2, & p+2, & 2p+2, & 3p+2, \dots \\ \vdots & & & & \\ K_{p-1}: & p-1, & 2p-1, & 3p-1, & 4p-1, \dots \end{array}$$

Wir definieren Addition und Multiplikation der Klassen nach dem Gesetz $K_a + K_b = K_s$, $K_a \cdot K_b = K_m$, wobei s und m die kleinsten positiven Reste mod p der Zahlen $a + b$ bezw. $a \cdot b$ bedeuten. Die Klassen $K_0, K_1, \dots, K_{p-1}$ oder ihre Repräsentanten, die Zahlen $0, 1, 2, \dots, p-1$, bilden ein endliches Feld von p Elementen. Man bezeichnet es auch als $GF[p]$.

Ein endliches Feld der Ordnung p^n (p Primzahl) läßt sich mittelst Kongruenzen durch ganze Funktionen einer Variablen mit ganzzahligen Koeffizienten einführen. Zwei ganze Funktionen $f(x)$ und $f_1(x)$ einer Variablen x mit ganzzahligen Koeffizienten heißen *kongruent* in bezug auf die Primzahl p,

wenn in der ganzen Funktion $f(x) - f_1(x)$ jeder Koeffizient durch die Primzahl p ohne Rest teilbar ist; alsdann schreibt man $f(x) \equiv f_1(x) \pmod{p}$. Für die hier vorliegenden Zwecke heißt eine ganze Funktion mit ganzzahligen Koeffizienten vom Grad n, wenn x^n die höchste Potenz ist, deren Koeffizient nicht durch p teilbar ist. Die ganze ganzzahlige Funktion $P(x)$ vom n^{ten} Grad, bei der x^n die Einheit als Koeffizient habe, heißt *irreduzibel*, falls keine Kongruenz $P(x) \equiv f_1(x) f_2(x) \pmod{p}$ möglich ist, wobei $f_1(x)$ und $f_2(x)$ ganze ganzzahlige Funktionen niederen als n^{ten} Grades bedeuten.

Jede ganze ganzzahlige Funktion $G(x)$ läßt sich vermittels der Funktion $P(x)$ in die Form:

$$G(x) = P(x)\,Q(x) + R(x)$$

bringen, wobei der Rest $R(x)$ eine ganze Funktion mit ganzzahligen Koeffizienten von niedrigerem als n^{tem} Grad ist. Sind $G_1(x)$ und $G_2(x)$ zwei ganze Funktionen mit ganzzahligen Koeffizienten und ihre durch Division mit $P(x)$ gewonnenen Reste $R_1(x)$ und $R_2(x)$ kongruent mod p, so werden $G_1(x)$ und $G_2(x)$ als *kongruent in bezug auf den Doppelmodul p, P* bezeichnet. Man schreibt

$$G_1(x) \equiv G_2(x) \pmod{p,\ P(x)}.$$

In bezug auf den Doppelmodul p, P zerfallen die ganzen Funktionen mit ganzzahligen Koeffizienten in p^n Klassen inkongruenter Funktionen; jede von diesen wird durch eine der p^n ganzen Funktionen:

$$t_0 + t_1 x + t_2 x^2 + \cdots + t_{n-1} x^{n-1}$$

repräsentiert; hierbei haben $t_0, t_1, t_2, \ldots, t_{n-1}$ die Reihe der Zahlen $0, 1, 2, \ldots, p-1$ *zu durchlaufen.* Addiert und multipliziert man die ganzen Funktionen mit ganzzahligen Koeffizienten, so ist sowohl ihre Summe als auch ihr Produkt einer der p^n angegebenen untereinander inkongruenten Funktionen kongruent in bezug auf den Doppelmodul (p, P). *Die p^n Klassen* mod (p, P) *inkongruenter ganzer Funktionen mit ganzzahligen Koeffizienten bilden ein endliches Feld von p^n Elementen.* Man bezeichnet es (E. H. Moore, *Math. papers of the Chicago Congress*, 1893, publ. 1896, S. 211) Galois zu Ehren, der (*Sur la théorie des nombres* (1830), *Œuvres*, p. 15) zuerst endliche Felder mit p^n Elementen verwendete, als $GF[p^n]$. Statt der

oben benützten p^n Funktionen kann man sich auch der von Galois a. a. O. eingeführten sogenannten *Galoisschen Imaginären* oder (H. Weber, *Algebra* **2**, 305) der Wurzeln der Gleichung $P = 0$ bedienen. Das $GF[p^n]$ ist Gegenstand des Werkes von L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Leipzig 1901, vgl. ferner J. A. Serret, *Algèbre supérieure*, Paris 1866, **2**, 121, de Séguier, *Éléments de la théorie des groupes abstraits*, Paris 1904, p. 28.

Ein endliches Feld von p^n Elementen liefert auch die Idealtheorie mittels Kongruenzen nach Primidealen n^{ten} Grades. Ist $\mathfrak{p}$ ein Primideal n^{ten} Grades im Körper $\mathfrak{K}$, also die Norm von $\mathfrak{p}$ gleich der n^{ten} Potenz der rationalen Primzahl p, so ist die Anzahl der nach dem Ideal $\mathfrak{p}$ untereinander inkongruenten ganzen Zahlen des Körpers $\mathfrak{K}$ gleich p^n. Diese p^n Zahlen bilden ein Feld mit p^n Elementen. Man kann auch stets einen Körper $\mathfrak{K}$ mit Primidealen $\mathfrak{p}$ finden, deren Norm einen vorgegebenen Wert p^n hat; im Kreiskörper der $p^n - 1^{\text{ten}}$ Einheitswurzeln ist nämlich die Primzahl p in Primideale n^{ten} Grades zerlegbar (vgl. Hilbert, *Die Theorie der algebraischen Zahlkörper, Math.-Ver.* (1897), Satz 125, S. 333).

Für die endlichen Felder gilt folgender Fundamentalsatz von E. H. Moore (*Math. papers of the Chicago Congress*, 1893, S. 220, L. E. Dickson, *Linear groups*, S. 13, E. H. Moore, *The decennial publications of the university of Chicago*, Vol. IX, S. 7, Chicago 1903): *Die Anzahl der verschiedenen Elemente irgendeines endlichen Feldes kann nur gleich einer Primzahl oder gleich einer ihrer Potenzen sein. Jedes mögliche endliche Feld hat in einem $GF[p^n]$ seinen Vertreter. Das $GF[p^n]$ ist unabhängig von der speziellen Wahl der irreduziblen Funktion $P(x)$; es wird durch p und n völlig charakterisiert* (letzteres Resultat eigentlich schon bei Galois, *Œuvres*, p. 17). Jedes endliche Feld $\mathfrak{C}$ mit p^n Elementen kann also mit jedem endlichen Feld $\mathfrak{C}'$ mit p^n Elementen derartig in eine eindeutige Beziehung gesetzt werden, daß, wenn a', b', c' Elemente aus $\mathfrak{C}'$ sind, die den Elementen a, b, c aus $\mathfrak{C}$ entsprechen, sich aus der Relation $a + b = c$ die Gleichung $a' + b' = c'$ und umgekehrt ergibt und aus $ab = c$ die Beziehung $a'b' = c'$ und umgekehrt folgt.

§ 2. Allgemeines über abstrakte Gruppen.

Eine Gruppe $\mathfrak{H}$ heißt eine *Untergruppe* (Lie, Netto, Frobenius), ein *Divisor* (Galois, *Œuvres,* p. 58) oder ein *echter Teiler* (Weber, *Algebra* 2, 7) einer Gruppe $\mathfrak{G}$, wenn sämtliche Elemente von $\mathfrak{H}$ auch der Gruppe $\mathfrak{G}$ angehören und $\mathfrak{G}$ außer den Elementen von $\mathfrak{H}$ wenigstens noch ein Element enthält.

Das Einheitselement ist eine Untergruppe jeder Gruppe. Ist A irgendein Element einer Gruppe $\mathfrak{G}$, so bilden die Elemente

$$\ldots A^{-2}, A^{-1}, A^0, A, A^2, \ldots$$

eine *zyklische Untergruppe von* $\mathfrak{G}$. Hat diese Reihe lauter verschiedene Elemente, so heißt A ein *Element unendlich hoher Ordnung.* Hat die obige Reihe nicht lauter untereinander verschiedene Elemente, so wird eine Potenz des Elementes A gleich dem Einheitselement. In diesem Falle heißt *das Element A von endlicher Ordnung.* Ist a die kleinste positive Zahl, für die $A^a = 1$ wird, so heißt a die *Ordnung* oder die *Periode des Elementes A.* (H. Weber, *Algebra* 2, 11 sagt Grad des Elementes A.)

Ist A ein Element der endlichen Ordnung a, so enthält die Reihe: $A^0, A^1, A^2, A^3, \ldots, A^{a-1}$ a voneinander verschiedene Elemente und erschöpft alle positiven wie negativen Potenzen von A. (Diese Sätze finden sich bereits bei Abel, vgl. *Ostwalds Klassiker d. exakten Wiss.* Nr. 111, S. 6.)

Alle Elemente, die zwei Gruppen $\mathfrak{G}_1$ und $\mathfrak{G}_2$ gemeinschaftlich angehören, bilden wiederum eine Gruppe; sie heißt der *größte gemeinschaftliche Teiler* oder nach Study (H. Weber, *Algebra* 2, 10) der *Durchschnitt von $\mathfrak{G}_1$ und $\mathfrak{G}_2$.* Zwei Gruppen, deren Durchschnitt nur aus dem Einheitselement besteht, heißen *teilerfremd.*

Die Gleichung $\mathfrak{A} = A + B + C + \cdots$ soll ausdrücken, die Elemente $A, B, C, \ldots$ sind zu einem System $\mathfrak{A}$ zusammengefaßt; die Gleichung

$$\mathfrak{K} = \mathfrak{A} + \mathfrak{B} + \mathfrak{C} + \cdots$$

bedeutet, die Systeme $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ sollen zu einem weiteren System $\mathfrak{K}$ vereinigt werden. Durchläuft A alle Elemente des Systems $\mathfrak{A}$ und B alle Elemente des Systems $\mathfrak{B}$, so durchläuft AB ein System von Elementen, das mit $\mathfrak{A}\mathfrak{B}$ bezeichnet sei.

Die Bildung $\mathfrak{A}\mathfrak{B}$ bezeichnet man als *Komposition von Systemen.* (H. Weber, *Algebra* 2, 13 spricht von der *Komposition der Teile.*) Besteht $\mathfrak{B}$ nur aus einem einzigen Element B, so wird $\mathfrak{A}B$ für $\mathfrak{A}\mathfrak{B}$ geschrieben; ebenso verwendet man, wenn $\mathfrak{A}$ nur aus einem einzigen Element A besteht, die Bezeichnung $A\mathfrak{B}$. Für *Gruppen* und *Systeme* werden im folgenden *große deutsche*, für *einzelne Elemente große lateinische Buchstaben* verwendet. (Vgl. hierzu Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 163.) Ein *Gleichheitszeichen* $\mathfrak{A} = \mathfrak{B}$ soll besagen, daß jedes Element des einen Systems auch in dem anderen vorkommt; hierbei soll jedoch nicht verlangt sein, daß in $\mathfrak{A}$ oder $\mathfrak{B}$ wiederholt auftretende Elemente sich in dem einen System ebenso häufig als in dem anderen vorfinden. $\mathfrak{A} > \mathfrak{B}$ besagt: Das System $\mathfrak{A}$ enthält alle Elemente von $\mathfrak{B}$, aber außerdem auch noch solche, die nicht in $\mathfrak{B}$ auftreten.

Zwei Systeme $\mathfrak{A}$ *und* $\mathfrak{B}$ *heißen vertauschbar, wenn* $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A}$ *ist, d. h. jedes Element des Systemes* $\mathfrak{A}\mathfrak{B}$ *in* $\mathfrak{B}\mathfrak{A}$ *auftritt und umgekehrt.*

Ein Element B heißt mit einem System $\mathfrak{A}$ *vertauschbar, wenn die Gleichung* $\mathfrak{A}B = B\mathfrak{A}$ *statthat.*

Jedes in einer Gruppe $\mathfrak{G}$ enthaltene Element G ist mit der Gruppe $\mathfrak{G}$ vertauschbar: $G\mathfrak{G} = \mathfrak{G}G$.

Sind $\mathfrak{G}_1$ und $\mathfrak{G}_2$ zwei Gruppen, so heißt die kleinste Gruppe $\mathfrak{C}$, die sowohl alle Elemente von $\mathfrak{G}_1$ als auch von $\mathfrak{G}_2$ umfaßt, *das kleinste gemeinsame Vielfache von* $\mathfrak{G}_1$ *und* $\mathfrak{G}_2$. Es ist $\mathfrak{C} \geqq \mathfrak{G}_1\mathfrak{G}_2$; das Gleichheitszeichen gilt dann und nur dann, wenn $\mathfrak{G}_1$ und $\mathfrak{G}_2$ vertauschbare Gruppen sind, also $\mathfrak{G}_1\mathfrak{G}_2 = \mathfrak{G}_2\mathfrak{G}_1$ ist. Eine Gruppe $\mathfrak{C}$, die zwei derartige Untergruppen $\mathfrak{G}_1$ und $\mathfrak{G}_2$ enthält, daß $\mathfrak{C} = \mathfrak{G}_1\mathfrak{G}_2 = \mathfrak{G}_2\mathfrak{G}_1$ ist, heißt *zerlegbar* (décomposable). Vgl. Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 166; E. Maillet, *Bull. soc. math.* 28, 7 (1900).

Sind $\mathfrak{G}_1$ und $\mathfrak{G}_2$ zwei teilerfremde Gruppen und ist jedes Element von $\mathfrak{G}_1$ mit jedem Element von $\mathfrak{G}_2$ vertauschbar, so heißt nach Hölder (*Math. Ann.* **34**, 36 (1889), ebenda **43**, 330 (1893)) das kleinste gemeinsame Vielfache $\mathfrak{C}$ von $\mathfrak{G}_1$ und $\mathfrak{G}_2$ das *direkte Produkt von* $\mathfrak{G}_1$ *und* $\mathfrak{G}_2$; die Gruppen $\mathfrak{G}_1$ und $\mathfrak{G}_2$ sind invariante Untergruppen von $\mathfrak{C}$. Eine Gruppe, die als direktes Produkt zweier Gruppen darstellbar ist, heißt *zerfallend.* (Dyck, *Math. Ann.* **17**, 482 (1880); Hölder, *Math. Ann.* **34**, 36 (1889), ebenda **43**, 335 (1893).) Zerfallende Gruppen sind eine spezielle Art zerlegbarer Gruppen.

$\mathfrak{H}_1$ und $\mathfrak{H}_2$ seien zwei gleiche oder verschiedene Gruppen, R irgendein Element. Betrachtet man das System $\mathfrak{H}_1 R \mathfrak{H}_2$ und ersetzt R durch irgendein anderes Element R', das dem System $\mathfrak{H}_1 R \mathfrak{H}_2$ angehört, so enthalten die zwei Systeme $\mathfrak{H}_1 R \mathfrak{H}_2$ und $\mathfrak{H}_1 R' \mathfrak{H}_2$ die nämlichen Elemente. Hieraus folgt: Haben zwei Systeme $\mathfrak{H}_1 R \mathfrak{H}_2$ und $\mathfrak{H}_1 S \mathfrak{H}_2$ ein Element gemeinsam, so stimmen sie in allen Elementen überein. Tritt das letztere ein, so heißen *die Elemente R und S äquivalent nach dem Doppelmodul* ($\mathfrak{H}_1$, $\mathfrak{H}_2$). Die Äquivalenz nach einem Doppelmodul ist eingeführt von Frobenius, *Journ. f. Math.* **101**, 273 (1887); vgl. ferner Dedekind, *Gött. Nachr.* (1894), 275, Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 167, H. Weber, *Algebra* **2**, 22, de Séguier, *Groupes abstraits,* S. 61.

Ist $\mathfrak{G}$ eine Gruppe mit den Untergruppen $\mathfrak{H}_1$ und $\mathfrak{H}_2$, so kann man $\mathfrak{G}$ in Systeme zerlegen:

$$(1) \qquad \mathfrak{G} = \mathfrak{H}_1 G_1 \mathfrak{H}_2 + \mathfrak{H}_1 G_2 \mathfrak{H}_2 + \mathfrak{H}_1 G_3 \mathfrak{H}_2 + \cdots;$$

hierbei haben niemals zwei auf der rechten Seite der Gleichung (1) stehende Systeme $\mathfrak{H}_1 G_i \mathfrak{H}_2$ und $\mathfrak{H}_1 G_k \mathfrak{H}_2$ ein Element gemeinsam. Die Elemente $G_1 = 1$, G_2, G_3, ... heißen ein *vollständiges System nicht äquivalenter Elemente* oder ein *vollständiges Restsystem der Gruppe* $\mathfrak{G}$ *nach dem Doppelmodul* ($\mathfrak{H}_1$, $\mathfrak{H}_2$); hierbei kann jedes Element G_i durch jedes andere Element von $\mathfrak{H}_1 G_i \mathfrak{H}_2$ ersetzt werden. Ist $\mathfrak{G}$ eine Gruppe mit einer nicht abzählbaren Menge von Elementen, so soll, wie bemerkt sei, durch die Numerierung und verwendete Schreibweise nicht etwa ausgedrückt werden, daß die Systeme $\mathfrak{H}_1 G_1 \mathfrak{H}_2$, $\mathfrak{H}_1 G_2 \mathfrak{H}_2$, $\mathfrak{H}_1 G_3 \mathfrak{H}_2$, ... eine im Sinn von G. Cantor abzählbare Menge sind.[1])

Gleichzeitig mit der Zerlegung (1) besteht die Zerlegung:

$$(2) \qquad \mathfrak{G} = \mathfrak{H}_2 G_1^{-1} \mathfrak{H}_1 + \mathfrak{H}_2 G_2^{-1} \mathfrak{H}_1 + \mathfrak{H}_2 G_3^{-1} \mathfrak{H}_1 + \cdots,$$

bei der die Systeme $\mathfrak{H}_2 G_i^{-1} \mathfrak{H}_1$ und $\mathfrak{H}_2 G_k^{-1} \mathfrak{H}_1$ niemals ein Element gemeinsam haben.

Wählt man bei der Zerlegung einer Gruppe nach einem aus zwei ihrer Untergruppen $\mathfrak{H}_1$ und $\mathfrak{H}_2$ gebildeten Doppel-

---

1) Diese Festsetzung, daß bei unendlich vielen Elementen im folgenden Numerierung und Punkte keine Abzählbarkeit im Sinne von G. Cantor bedeuten sollen, soll für unsere Betrachtungen allgemein gelten.

modul für die Gruppe $\mathfrak{H}_2$ das Einheitselement, das ja für sich allein eine Gruppe bildet, so geht die Zerlegung (1) in die bereits von *Galois* (*Œuvres*, p. 26) studierte über:

$$(1') \qquad \mathfrak{G} = \mathfrak{H}_1 G_1 + \mathfrak{H}_1 G_2 + \mathfrak{H}_1 G_3 + \cdots;$$

hierbei haben niemals zwei Systeme $\mathfrak{H}_1 G_i$ und $\mathfrak{H}_1 G_k$ ein Element gemeinsam. Die Elemente $G_1 = 1, G_2, G_3, \ldots$ heißen *ein vollständiges System nicht äquivalenter Elemente* oder ein *vollständiges Restsystem der Gruppe* $\mathfrak{G}$ *nach dem Modul* $\mathfrak{H}_1$. In dem Restsystem kann jedes Element G_i $(i = 1, 2, 3, \ldots)$ durch jedes andere Element des Systemes $\mathfrak{H}_1 G_i$ ersetzt werden. Trotzdem nur $\mathfrak{H}_1 G_1 = \mathfrak{H}_1$ eine Gruppe ist, bezeichnet man die Systeme $\mathfrak{H}_1 G_i$ $(i = 1, 2, 3, \ldots)$ nach H. Weber, *Algebra* **2**, 8 als ein *System von Nebengruppen* und spricht von *einer Zerlegung von* $\mathfrak{G}$ *in ein System von Nebengruppen.*

Gleichzeitig mit der Zerlegung (1′) besteht die Zerlegung:

$$(2') \qquad \mathfrak{G} = G_1^{-1}\mathfrak{H}_1 + G_2^{-1}\mathfrak{H}_1 + G_3^{-1}\mathfrak{H}_1 + \cdots,$$

bei der zwei Systeme $G_i^{-1}\mathfrak{H}_1$ und $G_k^{-1}\mathfrak{H}_1$ niemals ein Element gemeinsam haben.

Ist bei der Zerlegung (1′) die Anzahl der Nebengruppen endlich, besteht also die Zerlegung:

$$(1'') \qquad \mathfrak{G} = \mathfrak{H}_1 G_1 + \mathfrak{H}_1 G_2 + \mathfrak{H}_1 G_3 + \cdots + \mathfrak{H}_1 G_j$$

und infolgedessen auch gleichzeitig:

$$(2'') \qquad \mathfrak{G} = G_1^{-1}\mathfrak{H}_1 + G_2^{-1}\mathfrak{H}_1 + G_3^{-1}\mathfrak{H}_1 + \cdots + G_j^{-1}\mathfrak{H}_1,$$

so heißt $\mathfrak{H}_1$ *eine Untergruppe von* $\mathfrak{G}$ *von endlichem Index* j *und* j *der Index der Untergruppe.* Existiert keine solche endliche Zahl j, so ist $\mathfrak{H}_1$ eine Untergruppe von *unendlichem Index.* (Poincaré, *Journ. de math.* (4) **3**, 409 (1887).)

Nach Poincaré (a. a. O.) heißen *zwei Gruppen meßbar*, wenn ihr Durchschnitt für jede von ihnen eine Untergruppe von endlichem Index ist.

Sind zwei Gruppen $\mathfrak{G}_1$ und $\mathfrak{G}_2$ mit einer und derselben dritten Gruppe $\mathfrak{G}$ meßbar, so sind $\mathfrak{G}_1$ und $\mathfrak{G}_2$ untereinander meßbar und auch der größte gemeinsame Teiler von $\mathfrak{G}$, $\mathfrak{G}_1$ und $\mathfrak{G}_2$ ist für jede der drei Gruppen eine Untergruppe von endlichem Index.

Ist $\mathfrak{F}$ eine Gruppe, $\mathfrak{G}$ eine Untergruppe von $\mathfrak{F}$ und $\mathfrak{H}$ eine Untergruppe von $\mathfrak{G}$, so gilt die Relation:

$$(\mathfrak{F}, \mathfrak{H}) = (\mathfrak{F}, \mathfrak{G}) \cdot (\mathfrak{G}, \mathfrak{H}),$$

wenn $(\mathfrak{F}, \mathfrak{H})$ (vgl. H. Weber, *Algebra* **2**, 9) der (endliche oder unendliche) Index der Untergruppe $\mathfrak{H}$ von $\mathfrak{F}$, und analog $(\mathfrak{F}, \mathfrak{G})$ bzw. $(\mathfrak{G}, \mathfrak{H})$ die Indices der Untergruppen $\mathfrak{G}$ von $\mathfrak{F}$ bzw. $\mathfrak{H}$ von $\mathfrak{G}$ bedeuten.

Ist $\mathfrak{G}_1$ eine beliebige Gruppe und R irgendein Element, das nicht $\mathfrak{G}_1$ anzugehören braucht, so bildet auch das System von Elementen $\mathfrak{G}_2 = R\mathfrak{G}_1 R^{-1}$ eine Gruppe. Man sagt: $\mathfrak{G}_2$ ist eine *transformierte Gruppe von* $\mathfrak{G}_1$ oder *durch Transformation aus* $\mathfrak{G}_1$ hervorgegangen. $\mathfrak{G}_2$ heißt mit $\mathfrak{G}_1$ *ähnlich* (dies ist die älteste an Cauchy anknüpfende Bezeichnung, so bei J. A. Serret, *Algèbre supérieure* **2**, 255 (Paris, 3ième éd., 1866), Netto, *Substitutionentheorie*, S. 47), *konjugiert, gleichberechtigt* (Klein, Math. Ann. **14**, 430 (1879)) oder *äquivalent*. Die gegebene Definition ist in $\mathfrak{G}_1$ und $\mathfrak{G}_2$ symmetrisch; denn aus $\mathfrak{G}_2 = R\mathfrak{G}_1 R^{-1}$ folgt $\mathfrak{G}_1 = R^{-1}\mathfrak{G}_2 R = R^{-1}\mathfrak{G}_2(R^{-1})^{-1}$. Zwei Gruppen, die mit einer dritten ähnlich sind, sind es untereinander.

Zwei Untergruppen $\mathfrak{H}_1$ und $\mathfrak{H}_2$ einer Gruppe $\mathfrak{G}$ heißen *in bezug auf* $\mathfrak{G}$ *ähnliche, konjugierte, gleichberechtigte* oder *äquivalente Untergruppen* von $\mathfrak{G}$, wenn es in $\mathfrak{G}$ wenigstens ein Element R gibt, daß die Gruppen $\mathfrak{H}_2$ und $R\mathfrak{H}_1 R^{-1}$ in ihren Elementen übereinstimmen. Die gegebene Definition ist in $\mathfrak{H}_1$ und $\mathfrak{H}_2$ symmetrisch gebaut; denn aus $\mathfrak{H}_2 = R\mathfrak{H}_1 R^{-1}$ folgt $\mathfrak{H}_1 = R^{-1}\mathfrak{H}_2 R = R^{-1}\mathfrak{H}_2(R^{-1})^{-1}$, und wegen des Gruppencharakters von $\mathfrak{G}$ ist R^{-1} als reziprokes Element von R in $\mathfrak{G}$ enthalten.

Statt in bezug auf $\mathfrak{G}$ ähnlicher oder konjugierter Untergruppen spricht man auch kurz von *ähnlichen* oder *konjugierten Untergruppen von* $\mathfrak{G}$. Dabei ist folgendes zu beachten: Ist $\mathfrak{F}$ eine Gruppe, die $\mathfrak{G}$ als Untergruppe enthält, so können zwei Untergruppen $\mathfrak{H}_1$ und $\mathfrak{H}_2$ von $\mathfrak{G}$ miteinander sehr wohl in bezug auf $\mathfrak{F}$ ähnlich sein, ohne daß es in bezug auf $\mathfrak{G}$ der Fall ist; zwei solche Gruppen $\mathfrak{H}_1$ und $\mathfrak{H}_2$ sind als ähnliche oder konjugierte Untergruppen von $\mathfrak{F}$, nicht aber als ähnliche oder konjugierte Untergruppen von $\mathfrak{G}$ zu bezeichnen.

Jede Untergruppe einer Gruppe $\mathfrak{G}$ ist in bezug auf $\mathfrak{G}$ mit sich selbst ähnlich. Zwei ähnliche Untergruppen einer Gruppe $\mathfrak{G}$,

die in bezug auf $\mathfrak{G}$ einer dritten Untergruppe von $\mathfrak{G}$ ähnlich sind, sind es auch untereinander. Transformiert man eine Untergruppe $\mathfrak{H}$ der Gruppe $\mathfrak{G}$ durch ein vollständiges Restsystem der Gruppe $\mathfrak{G}$ nach dem Modul $\mathfrak{H}$, so erhält man alle mit $\mathfrak{H}$ in bezug auf $\mathfrak{G}$ ähnlichen Untergruppen von $\mathfrak{G}$, diese brauchen nicht alle voneinander verschieden zu sein. Ist $\mathfrak{H}$ im besondern eine Untergruppe von $\mathfrak{G}$ von endlichem Index, so ist die Anzahl der verschiedenen in bezug auf $\mathfrak{G}$ ähnlichen Untergruppen jedenfalls endlich.

Auch für die *einzelnen Elemente* einer Gruppe ist der Begriff der Ähnlichkeit zu definieren: *Zwei Elemente* A und B einer Gruppe $\mathfrak{G}$ heißen *in bezug auf* $\mathfrak{G}$ *ähnlich, konjugiert, gleichberechtigt* oder *äquivalent*, falls es in $\mathfrak{G}$ wenigstens ein Element C gibt, daß $A = CBC^{-1}$ wird. Wie aus $B = C^{-1}AC = C^{-1}A(C^{-1})^{-1}$ folgt, ist die gegebene Definition, da $\mathfrak{G}$ infolge seines Gruppencharakters neben jedem Element C auch das reziproke C^{-1} enthält, in A und B symmetrisch. Von dem Produkt CBC^{-1} sagt man: es ist *durch Transformation aus B hervorgegangen*.

Jedes Gruppenelement ist mit sich selbst ähnlich. Sind A_1 und A_2 zwei beliebige Elemente einer Gruppe $\mathfrak{G}$, so sind die zwei Produkte $A_1 A_2$ und $A_2 A_1 = A_2(A_1 A_2)A_2^{-1}$ miteinander in bezug auf $\mathfrak{G}$ ähnlich.

Zwei Gruppenelemente von $\mathfrak{G}$, die in bezug auf $\mathfrak{G}$ mit einem dritten ähnlich sind, sind es auch untereinander. Hieraus folgt: Alle mit einem Element einer Gruppe $\mathfrak{G}$ in bezug auf $\mathfrak{G}$ ähnlichen Elemente bilden eine Klasse ähnlicher Elemente, so daß zwei Elemente derselben Klasse stets untereinander ähnlich sind. Die Elemente einer Gruppe lassen sich also in *Klassen konjugierter Elemente* einteilen. (Frobenius, *Journ. f. Math.* **100**, 181 (1887).)

Sind C_1 und C_2 zwei in $\mathfrak{G}$ enthaltene Elemente, die beide bewirken, daß $C_1 A C_1^{-1} = B$ und $C_2 A C_2^{-1} = B$ wird, so ist $C_1^{-1} C_2 A = A C_1^{-1} C_2$, d. h. das in $\mathfrak{G}$ befindliche Element $C_1^{-1} C_2$ ist mit A vertauschbar. Hieraus folgt: Sind A und B zwei in bezug auf die Gruppe $\mathfrak{G}$ ähnliche Elemente von $\mathfrak{G}$, d. h. zwei Elemente derselben Klasse, so sind alle in $\mathfrak{G}$ enthaltenen Elemente X, die bewirken, daß $XAX^{-1} = B$ wird, von der Form $C_1 \mathfrak{B}$, wobei $\mathfrak{B}$ das System aller mit A vertauschbaren Elemente von $\mathfrak{G}$ bedeutet.

Ist A irgendein Element einer Gruppe $\mathfrak{G}$, *so bilden alle in* $\mathfrak{G}$ *enthaltenen, mit A vertauschbaren Elemente eine Gruppe.*

Das System 𝔙 ist also eine Gruppe, und man kann die Gruppe 𝔊 mit Galois nach dem Modul 𝔙 zerlegen:

$$\mathfrak{G} = \mathfrak{V} G_1 + \mathfrak{V} G_2 + \mathfrak{V} G_3 + \cdots$$

Hieraus ergibt sich: *Die Klasse der mit einem Element A einer Gruppe 𝔊 in bezug auf dieses ähnlichen Gruppenelemente besteht aus den Elementen:* A, $G_2 A G_2^{-1}$, $G_3 A G_3^{-1}$, ..., *die sämtlich untereinander verschieden sind.* $G_1 = 1$, G_2, G_3, ... *bedeuten ein vollständiges Restsystem der Gruppe 𝔊 nach dem Modul 𝔙; hierbei ist 𝔙 die Gruppe aller in 𝔊 enthaltenen, mit dem Element A vertauschbaren Elemente. Ist also im besonderen 𝔙 in bezug auf 𝔊 von endlichem Index j, so gibt es innerhalb 𝔊 genau j mit A ähnliche Gruppenelemente.*

Unter Umständen kann auch ein Element A einer Gruppe 𝔊 mit allen Elementen von 𝔊 vertauschbar sein; in diesem Fall fällt 𝔙 mit 𝔊 zusammen. Derartige Elemente sind nur mit sich selbst ähnlich, die Zahl j ist gleich 1. Solche Elemente einer Gruppe 𝔊, die mit jedem Element von 𝔊 vertauschbar sind, heißen *invariante, ausgezeichnete* oder *isolierte* (H. Weber, *Algebra* **2**, 133) *Gruppenelemente.* Das Einheitselement ist invariantes Element jeder Gruppe.

Ist eine Untergruppe 𝔋 von 𝔊 mit allen ihren in bezug auf 𝔊 ähnlichen Untergruppen identisch, so heißt 𝔋 eine *invariante* (Lie, *Math. Ann.* **25**, 77 (1885), nach der dortigen Angabe zuerst eingeführt *Arch. for Math. og. Naturw.* **3**, 457 (1878)) oder eine *ausgezeichnete* (Lie, auf den dieser Ausdruck zurückgeführt wird, lehnt ihn *Math. Ann.* **25**, 77 (1885) ab, die englische Bezeichnung „self-conjugate subgroup" ist als Übersetzung von „ausgezeichneter Untergruppe" von Cole, *Am. J. math.* **9**, 51 (1887) eingeführt worden) oder ein *Normalteiler* (H. Weber, *Algebra* **2**, 12) oder ein *eigentlicher Teiler* von 𝔊.

Eine invariante Untergruppe 𝔋 von 𝔊 kann auch dadurch definiert werden, daß alle Elemente von 𝔊 mit 𝔋 vertauschbar sind, also für jedes Element G von 𝔊 die Gleichung $G\mathfrak{H} = \mathfrak{H}G$ *stattfinden muß.*

Der Begriff der invarianten Untergruppe ist einer der wichtigsten der ganzen Gruppentheorie; man verdankt ihn Galois. Er spricht, wenn die Zerlegungen

$$\mathfrak{G} = \mathfrak{H}G_1 + \mathfrak{H}G_2 + \mathfrak{H}G_3 + \cdots$$

und

$$\mathfrak{G} = G_1\mathfrak{H} + G_2\mathfrak{H} + G_3\mathfrak{H} + \cdots$$

identisch sind, von einer décomposition propre (*Œuvres,* p. 26); $G_1 = 1, G_2, G_3, \ldots$ bedeuten ein vollständiges Restsystem der Gruppe $\mathfrak{G}$ nach dem Modul $\mathfrak{H}$. Anknüpfend an die Galoissche Ausdrucksweise ist die Bezeichnung „eigentlicher Teiler" (Dedekind, *Math. Ann.* **48**, 548 (1897)) entstanden.

Das Einheitselement ist eine invariante Untergruppe jeder Gruppe. Der Durchschnitt aller mit einer Untergruppe $\mathfrak{H}$ einer Gruppe $\mathfrak{G}$ in bezug auf $\mathfrak{G}$ ähnlichen Gruppen ist eine invariante Untergruppe von $\mathfrak{G}$.

Ist $\mathfrak{H}$ eine Untergruppe von $\mathfrak{G}$, $\mathfrak{K}$ eine Untergruppe von $\mathfrak{H}$ und $\mathfrak{K}$ invariante Untergruppe von $\mathfrak{G}$, so ist $\mathfrak{K}$ auch invariante Untergruppe von $\mathfrak{H}$.

Sind $\mathfrak{H}_1$ und $\mathfrak{H}_2$ zwei invariante Untergruppen von $\mathfrak{H}$, so ist ihr Durchschnitt $\mathfrak{D}$ eine invariante Untergruppe von $\mathfrak{H}$, $\mathfrak{H}_1$ und $\mathfrak{H}_2$.

Die Gesamtheit der invarianten Elemente einer Gruppe $\mathfrak{G}$ bildet eine invariante Untergruppe von $\mathfrak{G}$; nach de Séguier, *Groupes abstraits*, S. 57 heißt sie die *Zentrale von* $\mathfrak{G}$. Nur bei einer kommutativen Gruppe, bei dieser aber auch stets, fällt die Zentrale einer Gruppe $\mathfrak{G}$ mit der ganzen Gruppe zusammen.

Jede invariante Untergruppe $\mathfrak{J}$ einer Gruppe $\mathfrak{G}$ bestimmt, wenn $\mathfrak{J}$ nicht das Einheitselement ist, eine neue Gruppe. Sie heißt die *Quotientengruppe von* $\mathfrak{G}$ *und* $\mathfrak{J}$ oder *die zu* $\mathfrak{J}$ *in bezug auf* $\mathfrak{G}$ *komplementäre Gruppe. Sie wird mit* $\mathfrak{G}/\mathfrak{J}$ *bezeichnet.* Man sagt: $\mathfrak{G}$ *ist aus den zwei Gruppen* $\mathfrak{G}/\mathfrak{J}$ *und* $\mathfrak{J}$ *zusammengesetzt. Man bezeichnet* $\mathfrak{G}/\mathfrak{J}$ *auch als Faktorgruppe.* Die Quotientengruppe $\mathfrak{G}/\mathfrak{J}$ ist von C. Jordan, *Bull. soc. math.* **1**, 46 (1873) eingeführt und von Hölder (*Math. Ann.* **34**, 33 (1889)) von neuem aufgestellt worden. Die Quotientengruppe $\mathfrak{G}/\mathfrak{J}$ wird auf folgende Weise gefunden: Man zerlege die Gruppe $\mathfrak{G}$ mittels der invarianten Untergruppe $\mathfrak{J}$ in ein System von Nebengruppen:

$$\mathfrak{G} = \mathfrak{J}G_1 + \mathfrak{J}G_2 + \mathfrak{J}G_3 + \cdots,$$

wobei $G_1 = 1, G_2, G_3, \ldots$ ein vollständiges Restsystem der Gruppe $\mathfrak{G}$ nach dem Modul $\mathfrak{J}$ bilden. Man betrachte die

Nebengruppen $\mathfrak{C}_s = \mathfrak{J} G_s$ $(s = 1, 2, 3, \ldots)$. Die Systeme $\mathfrak{C}_s$ bilden, wenn man sie komponiert, eine Gruppe; ihr Einheitselement ist $\mathfrak{C}_1$. Das Produkt $\mathfrak{C}_k \cdot \mathfrak{C}_l$ zweier Nebengruppen enthält genau die gleichen Elemente wie eine bestimmte Nebengruppe $\mathfrak{C}_m$, so daß $\mathfrak{C}_k \cdot \mathfrak{C}_l = \mathfrak{C}_m$ wird; die Produktbildung ist für die Systeme $\mathfrak{C}$ assoziativ, schließlich sind $\mathfrak{C}_s = \mathfrak{J} G_s$ und $\mathfrak{J} G_s^{-1}$ reziproke Elemente der Gruppe $\mathfrak{G}/\mathfrak{J}$.

Enthält eine Gruppe $\mathfrak{G}$ außer dem Einheitselement keine invariante Untergruppe, so heißt die Gruppe $\mathfrak{G}$ *einfach*. Eine nicht einfache Gruppe heißt *zusammengesetzt*. Zu jeder zusammengesetzten Gruppe $\mathfrak{G}$ gibt es wenigstens eine Quotientengruppe $\mathfrak{G}/\mathfrak{J}$. Der fundamentale Begriff der einfachen Gruppe ist von Galois eingeführt worden. Er spricht von einer „groupe indécomposable" (*Œuvres*, p. 26).

Eine invariante Untergruppe $\mathfrak{J}$ einer Gruppe $\mathfrak{G}$, die in keiner größeren invarianten Untergruppe von $\mathfrak{G}$ enthalten ist, heißt eine *größte invariante* oder eine *invariante Maximal-Untergruppe* oder ein *größter Normalteiler* oder eine *ausgezeichnete Maximal-Untergruppe von* $\mathfrak{G}$.

Eine Gruppe $\mathfrak{J}$ ist dann und nur dann eine größte invariante Untergruppe einer Gruppe $\mathfrak{G}$, wenn die Quotientengruppe $\mathfrak{G}/\mathfrak{J}$ einfach ist.

Sind $\mathfrak{J}_1$ *und* $\mathfrak{J}_2$ *zwei größte invariante Untergruppen von* $\mathfrak{G}$, *so ist der Durchschnitt* $\mathfrak{D}$ *von* $\mathfrak{J}_1$ *und* $\mathfrak{J}_2$ *sowohl größte invariante Untergruppe von* $\mathfrak{J}_1$ *als auch von* $\mathfrak{J}_2$. *Die Faktorgruppen* $\mathfrak{G}/\mathfrak{J}_1$ *und* $\mathfrak{J}_2/\mathfrak{D}$ *sind holoedrisch isomorph* (vgl. unten); *das gleiche trifft für die Faktorgruppen* $\mathfrak{G}/\mathfrak{J}_2$ *und* $\mathfrak{J}_1/\mathfrak{D}$ *zu.*

Die Gruppe $\mathfrak{G}/\mathfrak{D}$ ist das direkte Produkt der zwei Gruppen $\mathfrak{J}_1/\mathfrak{D}$ und $\mathfrak{J}_2/\mathfrak{D}$. (Vgl. hierzu Hölder, *Math. Ann.* **34**, 36 (1889), Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 169). Der Begriff der größten invarianten Untergruppe einer Gruppe findet sich bei C. Jordan, *Journ. de math.* (2) **14**, 139 (1869), *Traité*, p. 41.

Eine invariante Untergruppe $\mathfrak{J}$ einer Gruppe $\mathfrak{G}$ heißt eine *charakteristische Untergruppe* von $\mathfrak{G}$, wenn $\mathfrak{J}$ nicht nur in $\mathfrak{G}$, sondern auch in jeder möglichen erweiterten Gruppe invariant ist, die $\mathfrak{G}$ als invariante Untergruppe enthält. Der Begriff der charakteristischen Untergruppe stammt von Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 183.

Zwei Gruppenelemente A und B bestimmen stets eindeutig ein drittes $A^{-1}B^{-1}AB$; dieses heißt der *Kommutator von A und B*. Die Gesamtheit der Kommutatoren einer Gruppe $\mathfrak{G}$ bildet im allgemeinen für sich keine Gruppe. Da aber nicht nur die Kommutatoren, sondern auch alle aus ihnen durch Produktbildung entstehenden Elemente ebenfalls in der Gruppe $\mathfrak{G}$ enthalten sind, so erzeugen die Kommutatoren, wenn man sie auf jede Weise komponiert, eine Gruppe $\mathfrak{K}$, die nur Elemente aus $\mathfrak{G}$ enthält. $\mathfrak{K}$ heißt die *Kommutatorgruppe* oder die *erste derivierte (abgeleitete) Gruppe von $\mathfrak{G}$*. *Die Gruppe $\mathfrak{K}$ ist nicht nur eine invariante, sondern sogar eine charakteristische Untergruppe von $\mathfrak{G}$.*

Ist die Kommutatorgruppe $\mathfrak{K}$ einer Gruppe $\mathfrak{G}$ mit $\mathfrak{G}$ identisch, so heißt $\mathfrak{G}$ eine *perfekte Gruppe.* Jede einfache Gruppe ist a fortiori eine perfekte Gruppe.

Die Kommutatorgruppe $\mathfrak{K}$ einer Gruppe $\mathfrak{G}$ enthält mindestens so viel verschiedene Elemente wie irgendeine Klasse konjugierter Elemente, wenn man $\mathfrak{G}$ in Klassen konjugierter Elemente einteilt. *Ist $\mathfrak{K}$ die Kommutatorgruppe einer Gruppe $\mathfrak{G}$, so ist $\mathfrak{G}/\mathfrak{K}$ eine kommutative Gruppe.* Ist $\mathfrak{J}$ irgendeine invariante Untergruppe von $\mathfrak{G}$, so ist $\mathfrak{G}/\mathfrak{J}$ dann und nur dann eine kommutative Gruppe, wenn $\mathfrak{J}$ die Kommutatorgruppe $\mathfrak{K}$ von $\mathfrak{G}$ zur Untergruppe hat.

Eine charakteristische Eigenschaft einer kommutativen Gruppe ist, daß ihre Kommutatorgruppe das Einheitselement ist.

Die Kommutatorgruppe hat ihren Ausgangspunkt in Lies Theorie der kontinuierlichen Gruppen, Lie-Engel, *Theorie der Transformationsgruppen* **3**, 678 und 770. Von dort, a. a. O., S. 679 stammt auch die Bezeichnung „perfekte Gruppe". Als Literatur über die Kommutatorgruppe ist zu nennen: G. A. Miller, *Quart. Journ.* **28**, 266 (1896), *Bull. Am. M. S.* **4**, 135 (1898), *Am. J* **20**, 277 (1898), G. Frobenius, *Sitzungsb. d. Berl. Akad.* (1896), 1348, Dedekind, *Math. Ann.* **48**, 553 (1897).

Zwei Gruppen $\mathfrak{G}$ und $\mathfrak{G}'$ heißen *holoedrisch isomorph, einfach isomorph, einstufig isomorph* oder kurz *isomorph*, wenn sich ihre Elemente $G_1, G_2, \ldots$ und $G_1', G_2', \ldots$ derartig gegenseitig eindeutig zuordnen lassen, daß, wenn zwei Elemente G_i' und G_k' der Gruppe $\mathfrak{G}'$ den Elementen G_i und G_k der Gruppe $\mathfrak{G}$ entsprechen, das Produkt $G_i'G_k'$ stets dem Produkt G_iG_k zugeordnet ist.

Sind $\mathfrak{G}$ und $\mathfrak{G}'$ isomorphe Gruppen, so ist jeder Untergruppe von $\mathfrak{G}$ eine Untergruppe von $\mathfrak{G}'$ isomorph zugeordnet, den Elementen von $\mathfrak{G}$ entsprechen in $\mathfrak{G}'$ Elemente der nämlichen Ordnung, dem Einheitselement von $\mathfrak{G}$ ist das Einheitselement von $\mathfrak{G}'$ zugeordnet.

Zwei zu einer dritten isomorphe Gruppen sind es nach der Definition des Isomorphismus auch stets untereinander. Jede Gruppe kann daher als Repräsentant aller mit ihr isomorphen Gruppen aufgefaßt werden. Eine spezielle Art des Isomorphismus ist die Ähnlichkeit. Zwei ähnliche Gruppen sind stets isomorph.

Man spricht von einem *meroedrischen Isomorphismus,* auch *mehrstufigen Isomorphismus* zwischen zwei Gruppen $\mathfrak{G}$ und $\mathfrak{G}'$, wenn zwischen ihren Elementen folgende Beziehung statthat: Jedem Element aus $\mathfrak{G}$ entspricht ein und auch nur ein Element aus $\mathfrak{G}'$, jedem Element aus $\mathfrak{G}'$ sind hierdurch ein oder auch mehrere Elemente aus $\mathfrak{G}$ zugeordnet; stets, wenn zwei Elemente G_i' und G_k' aus $\mathfrak{G}'$ den Elementen G_i und G_k aus $\mathfrak{G}$ entsprechen, soll das Produkt $G_i' G_k'$ dem Produkt $G_i G_k$ zugeordnet sein.

Diejenigen Elemente von $\mathfrak{G}$, die dem Einheitselement von $\mathfrak{G}'$ entsprechen, bilden eine invariante Untergruppe $\mathfrak{J}$ von $\mathfrak{G}$. Zerlegt man die Gruppe $\mathfrak{G}$ mit Hilfe der invarianten Untergruppe $\mathfrak{J}$:

$$\mathfrak{G} = \mathfrak{J}G_1 + \mathfrak{J}G_2 + \mathfrak{J}G_3 + \cdots,$$

wobei $G_1, G_2, G_3, \ldots$ ein vollständiges Restsystem der Gruppe $\mathfrak{G}$ nach dem Modul $\mathfrak{J}$ bilden, und entsprechen die Elemente $G_1', G_2', G_3', \ldots$ von $\mathfrak{G}'$ den Elementen $G_1, G_2, G_3, \ldots$ von $\mathfrak{G}$, so ist mit ihnen $\mathfrak{G}'$ erschöpft und allen Elementen des Systemes $\mathfrak{J}G_i$ aus $\mathfrak{G}$ entspricht das Element G_i'. *Die Faktorgruppe* $\mathfrak{G}/\mathfrak{J}$ *ist mit* $\mathfrak{G}'$ *holoedrisch isomorph.*

Die Gruppe $\mathfrak{G}$ heißt mehrstufig oder mehrfach (multiply) isomorph zu $\mathfrak{G}'$ (so bei H. Weber, *Algebra* 2, 18 sowie bei W. Burnside, *Theory of groups,* S. 36, nach Netto, *Substitutionentheorie,* S. 97, wo der Ausdruck „mehrstufiger Isomorphismus" eingeführt ist, wären $\mathfrak{G}'$ und $\mathfrak{G}$ zu vertauschen), $\mathfrak{G}'$ heißt meroedrisch isomorph zu $\mathfrak{G}$. Enthält $\mathfrak{J}$ unendlich viele Elemente, so sagt man: $\mathfrak{G}$ ist mit $\mathfrak{G}'$ ∞-stufig isomorph. Ist $\mathfrak{J}$ eine endliche Gruppe der Ordnung i, so spricht man von einem i-stufigen Isomorphismus. Der holoedrische und meroedrische Isomorphismus sind, und zwar unter dieser Bezeichnung, eingeführt von C. Jordan, *Traité,* p. 56.

Eine noch *weitergehende Definition des Isomorphismus* als die eben gegebene erhält man nach Capelli, *Giorn. di mat.* **16**, 33 (1878), wenn man die Bedingung fallen läßt, daß jedem Element aus $\mathfrak{G}$ nur *ein einziges* Element aus $\mathfrak{G}'$ entsprechen soll. Zwei Gruppen heißen *allgemein isomorph,* wenn für sie eine derartige wechselseitige Beziehung der Elemente definiert ist, daß jedem Element der einen Gruppe eines oder mehrere der andern Gruppe entsprechen, und falls den Elementen G_i und G_k aus $\mathfrak{G}$ die Elemente G_i' und G_k' aus $\mathfrak{G}'$ entsprechen, auch $G_i G_k$ und $G_i' G_k'$ entsprechende Elemente sind. Sind $\mathfrak{J}_1$, bezw. $\mathfrak{J}_1'$ die Systeme von Elementen aus $\mathfrak{G}$ bezw. $\mathfrak{G}'$, die dem Einheitselement aus $\mathfrak{G}'$ bezw. aus $\mathfrak{G}$ entsprechen, so sind $\mathfrak{J}_1$ und $\mathfrak{J}_1'$ nicht mehr notwendig Gruppen, sondern *Halbgruppen* (Dickson, *Trans. Am. M. S.* **6**, 207 (1905)). Ist eine der Halbgruppen $\mathfrak{J}_1$ oder $\mathfrak{J}_1'$ eine Gruppe, so ist es auch die andere. Sind $\mathfrak{J}_1$ und $\mathfrak{J}_1'$ Gruppen, so sind sie invariante Untergruppen von $\mathfrak{G}$ bezw. $\mathfrak{G}'$ und die Quotientengruppen $\mathfrak{G}/\mathfrak{J}_1$ und $\mathfrak{G}'/\mathfrak{J}_1'$ sind holoedrisch isomorph. (Vgl. Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 169, de Séguier, *Groupes abstraits,* S. 66.)

Irgendein System $\mathfrak{S}$ von Elementen $A, B, C, \ldots,$ die untereinander komponiert werden können, bildet eine *Halbgruppe* (de Séguier, *Groupes abstraits,* S. 8, Dickson, *Trans. Am. M. S.* **6**, 205 (1905)), wenn es die folgenden vier voneinander unabhängigen Postulate erfüllt:

1. Das Produkt irgend zweier Elemente von $\mathfrak{S}$ gehört $\mathfrak{S}$ an.
2. Die Produktbildung ist assoziativ.

3. und 4. Sind G, X und Y irgend drei Elemente aus $\mathfrak{S}$ und ist $GX = GY$ oder $XG = YG$, so soll in jedem der beiden Fälle die Gleichheit $X = Y$ stattfinden.

Eine Halbgruppe mit einer endlichen Anzahl von Elementen ist eine Gruppe. (Vgl. die Definition einer endlichen Gruppe bei H. Weber, *Math. Ann.* **20**, 302 (1882), *Algebra* **2**, 3, Frobenius, *Journ. f. Math.* **100**, 179 (1887).) Eine Halbgruppe braucht nicht das Einheitselement und nicht zu jedem Element das reziproke zu enthalten. Für eine Halbgruppe $\mathfrak{S}$ gilt die symbolische Gleichung $\mathfrak{S}^2 \leqq \mathfrak{S}$, während für eine Gruppe $\mathfrak{S}^2 = \mathfrak{S}$ ist; es gibt auch Halbgruppen, für die $\mathfrak{S}^2 = \mathfrak{S}$ ist.

Für jede Art des Isomorphismus, der hierbei seiner Natur nach unbestimmt gelassen wird, bürgert sich nach F. Klein, *Math. Ann.* **41**, 22 (1893) mehr und mehr die Bezeichnung *Homomorphismus* ein; man beschränkt das Wort „Isomorphismus“ dann auf den holoedrischen Isomorphismus. Bezeichnet man im Fall

des meroedrischen Isomorphismus die Gruppen wie früher mit $\mathfrak{G}$ und $\mathfrak{G}'$, so sagt man: $\mathfrak{G}$ ist zu $\mathfrak{G}'$ mehrfach homomorph, $\mathfrak{G}'$ ist mit $\mathfrak{G}$ meroedrisch homomorph. (Vgl. hierzu Burkhardt, *Enzykl. d. math. Wiss.* **1**, 217, de Séguier, *Groupes abstraits*, S. 66.)

Läßt man die Elemente einer Gruppe $\mathfrak{G}$ einfach isomorph sich selbst in anderer Reihenfolge entsprechen, so bezeichnet man eine solche Zuordnung als einen *Isomorphismus der Gruppe in sich selbst.* Man spricht auch von einem *Automorphismus* (Frobenius, *Sitzungsb. d. Berl. Akad.* (1901), 1324), oder von einem *Holomorphismus* (G. A. Miller, *Bull. Am. M. S.* (2) **9**, 112 (1902)). Ein Automorphismus einer Gruppe $\mathfrak{G}$ entsteht beispielsweise, wenn jedem Element G_i aus $\mathfrak{G}$ das Element $B^{-1}G_iB$ zugeordnet wird, wobei B irgendein festes, nicht invariantes Element aus $\mathfrak{G}$ bedeutet. Ein Automorphismus, der sich auf die eben geschilderte Art erzeugen läßt, heißt ein *innerer Automorphismus* oder ein *kogredienter Isomorphismus.* Existieren noch andere Automorphismen, so werden sie als *äußere Automorphismen* oder *kontragrediente Isomorphismen* bezeichnet.

Die Gesamtheit der Automorphismen einer Gruppe hat selbst Gruppencharakter; diese Gruppe heißt die *Isomorphismengruppe* (*i*-group bei englischen Autoren). *Die inneren Automorphismen bilden eine invariante Untergruppe der Isomorphismengruppe. Ist $\mathfrak{C}$ die Zentrale von $\mathfrak{G}$, so ist die Gruppe der inneren Automorphismen von $\mathfrak{G}$ holoedrisch isomorph mit der Gruppe $\mathfrak{G}/\mathfrak{C}$.*

Sind $G_1, G_2, G_3, \ldots$ die Elemente einer Gruppe $\mathfrak{G}$ und entspricht G_i bei einem Automorphismus der Gruppe $\mathfrak{G}$ das Element G_i' von $\mathfrak{G}$, so kann:

$$\begin{pmatrix} G_1 & G_2 & G_3 & \ldots \\ G_1' & G_2' & G_3' & \ldots \end{pmatrix}$$

als Permutation aufgefaßt werden; sie bezieht sich auf unendlich viele oder auf eine endliche Anzahl von Symbolen, je nachdem $\mathfrak{G}$ eine unendliche oder eine endliche Anzahl von Elementen besitzt. Die Isomorphismengruppe besteht aus der Gesamtheit aller dieser Permutationen.

Die Hervorhebung der Wichtigkeit der Isomorphismengruppe beginnt mit Hölder, *Math. Ann.* **43**, 313 (1893) und E. H. Moore, *Bull. Am. M. S.* (2) **1**, 61 (1895), die voneinander unabhängig auf die Isomorphismengruppe kamen. (Vgl. Moore, ebenda (2) **2**, 33 (1896).) Die Unterscheidung zwischen kogredienten

und kontragredienten Isomorphismen hatte Klein bereits bei dem speziellen Fall der Ikosaedergruppe in seinen *Vorlesungen über das Ikosaeder*, S. 232, gewonnen. Von Lehrbüchern vgl. über die Isomorphismengruppe: Burnside, *Theory of groups*. S. 221 ff.

Alle Elemente einer Gruppe $\mathfrak{G}$ können unter Umständen dadurch entstehen, daß man eine endliche Anzahl von Gruppenelementen $S_1, S_2, \ldots, S_q$ auf jede mögliche Weise untereinander komponiert. In diesem Fall sagt man: *die Gruppe $\mathfrak{G}$ wird von den q Elementen $S_1, S_2, \ldots, S_q$ erzeugt*. Die Elemente $S_1, S_2, \ldots S_q$ heißen ein *System erzeugender Elemente der Gruppe*. Enthält das System $S_1, S_2, \ldots, S_q$ keine überflüssigen Elemente, d. h. ist kein Element S_i $(i = 1, 2, \ldots, q)$ durch Komposition aus den $(q-1)$ übrigen S zu erhalten, so heißen $S_1, S_2, \ldots, S_q$ ein *System unabhängiger erzeugender Elemente der Gruppe $\mathfrak{G}$*. Jede Gleichung, die zwischen ausschließlich unabhängigen erzeugenden Elementen von $\mathfrak{G}$ und der Einheit besteht, heißt eine *fundamentale Definitionsgleichung* der Gruppe; sie läßt sich stets in der Form:

$$f(S) = S_{\alpha_1}^{\lambda_1} S_{\alpha_2}^{\lambda_2} \cdots S_{\alpha_\tau}^{\lambda_\tau} = 1$$

voraussetzen; hierbei sind $\lambda_1, \lambda_2, \ldots \lambda_\tau$ ausschließlich positive Zahlen und $\alpha_1, \alpha_2, \ldots, \alpha_\tau$ Zahlen aus der Reihe $1, 2, \ldots, q$, die beliebig häufig auftreten können $(\tau \gtreqless q)$. Die Gesamtheit fundamentaler Definitionsgleichungen, bei denen diejenigen, die aus den anderen folgen, fortgelassen werden können, heißt *ein System definierender Gleichungen* oder die *Gleichungen der Gruppe*. Durch ein System unabhängiger erzeugender Elemente und ein System definierender Gleichungen ist das Gesetz der Multiplikation irgend zweier Gruppenelemente bekannt und hiermit die Gruppe völlig eindeutig definiert. Da jede Gruppe neben jedem Element das reziproke enthalten muß, findet zwischen den erzeugenden Elementen einer Gruppe stets wenigstens eine Definitionsgleichung statt.

Eine zyklische endliche Gruppe der Ordnung n wird durch ein Element S_1 und die Gleichung $S_1^n = 1$ festgelegt, eine unendliche zyklische Gruppe ist durch zwei unabhängige Elemente S_1, S_2 und die Definitionsgleichung $S_1 S_2 = 1$ bestimmt.

Jede endliche Gruppe läßt sich durch eine endliche Anzahl von Elementen erzeugen, nicht aber jede unendliche Gruppe. Unsere gewöhnlichen rationalen Zahlen bilden bei Ausschluß der

Null bezüglich der Multiplikation eine kommutative Gruppe; wie aus dem Euclidschen Satz von der Existenz unendlichvieler Primzahlen folgt, kann diese Gruppe nicht durch eine endliche Anzahl von Elementen erzeugt werden. In der Theorie der linearen homogenen Differentialgleichungen spielen Gruppen, die durch eine endliche Anzahl von Elementen erzeugt werden, eine fundamentale Rolle. Vgl. L. Schlesinger, *Handbuch der Theorie der Differentialgleichungen*, 2_1, Leipzig 1897, S. 11.

Die denkbar einfachste Gruppe, die von q unabhängigen Elementen $S_1, S_2, \ldots, S_q$ erzeugt wird, ist die unendliche Gruppe $\mathfrak{G}$, bei der zwischen den Elementen die einzige Gleichung $S_1 S_2 \ldots S_q = 1$ besteht. $\overline{\mathfrak{G}}$ sei eine Gruppe, die von den q unabhängigen Elementen $\overline{S}_1, \overline{S}_2, \ldots, \overline{S}_q$ erzeugt wird. Befriedigen diese außer der Relation $\overline{S}_1 \overline{S}_2 \ldots \overline{S}_q = 1$ noch das System der definierenden Gleichungen $f_1(\overline{S}) = 1$, $f_2(\overline{S}) = 1, \ldots, f_n(\overline{S}) = 1$, so ist die Gruppe $\overline{\mathfrak{G}}$ mit der Gruppe $\mathfrak{G}/\mathfrak{J}$ holoedrisch isomorph. Die Gruppe $\mathfrak{J}$ entsteht, wenn man alle Operationen $R^{-1} f_i(S) R$ $(i = 1, 2, \ldots, n)$ der Gruppe $\mathfrak{G}$ auf jede Art komponiert; R bedeutet jedes Element aus $\mathfrak{G}$. Diese Untersuchungen stammen von W. Dyck, *Math. Ann.* **20**, 1 (1882) u. **22**, 70 (1883), ihnen parallel gehen geometrische Darstellungen einer Gruppe durch Einteilung von Bereichen in gleichartige Gebiete. Von Lehrbüchern vgl. W. Burnside, *Theory of groups*, S. 255 bis 310.

§ 3. Abstrakte endliche Gruppen.

Besonders weitreichend werden viele Sätze des vorigen Paragraphen, wenn man sie auf endliche Gruppen anwendet. Um die Ordnung g einer endlichen Gruppe $\mathfrak{G}$ zum Ausdruck zu bringen, schreibt man $\mathfrak{G}_g$.

Fundamentalsatz für endliche Gruppen ist der *Satz von Lagrange* (*Réflexions sur la résolution algébrique des équations* (1770), *Œuvres* **3**): *Jede Untergruppe $\mathfrak{H}$ einer endlichen Gruppe $\mathfrak{G}$ ist selbst eine endliche Gruppe und die Ordnung h von $\mathfrak{H}$ ist ein Divisor der Ordnung g von $\mathfrak{G}$. Der Quotient $j = \frac{g}{h}$, den man mit $(\mathfrak{G}, \mathfrak{H})$ bezeichnet, heißt der Index der Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$.*

Der Satz von Lagrange ist eine unmittelbare Folge der Zerlegung der Gruppe $\mathfrak{G}$ in ein System von Nebengruppen. (Vgl. Gleichung (1′) auf S. 183.) Aus dem Satz von Lagrange folgt: *Eine endliche Gruppe enthält nur Elemente von endlicher Ord-*

nung, und die Ordnung jedes Elementes ist ein Divisor der Gruppenordnung.

Bei einer endlichen Gruppe $\mathfrak{G}$ mit den Untergruppen $\mathfrak{H}_1$ und $\mathfrak{H}_2$ erreicht die Zerlegung von $\mathfrak{G}$ nach dem Doppelmodul $(\mathfrak{H}_1, \mathfrak{H}_2)$ stets ihr Ende. Die Gleichung (1) auf S. 182 nimmt die Form an: $\mathfrak{G} = \mathfrak{H}_1 G_1 \mathfrak{H}_2 + \mathfrak{H}_1 G_2 \mathfrak{H}_2 + \cdots + \mathfrak{H}_1 G_l \mathfrak{H}_2$. Es wird: $(\mathfrak{G}, \mathfrak{H}_1) = (\mathfrak{H}_2, \mathfrak{D}_1) + (\mathfrak{H}_2, \mathfrak{D}_2) + \cdots + (\mathfrak{H}_2, \mathfrak{D}_l)$. $(\mathfrak{G}, \mathfrak{H}_1)$ ist der Index $\frac{g}{h_1}$ der Untergruppe $\mathfrak{H}_1$ von $\mathfrak{G}$; $(\mathfrak{H}_2, \mathfrak{D}_i)$ ist der Index $\frac{h_2}{d_i}$ der Untergruppe $\mathfrak{D}_i$ von $\mathfrak{H}_2$; hierbei ist $\mathfrak{D}_i$ $(i = 1, 2, \ldots, l)$ der Durchschnitt der zwei Gruppen $\mathfrak{H}_2$ und $G_i^{-1} \mathfrak{H}_1 G_i$. (Satz von Frobenius, *Journ. f. Math.* **101**, 281 (1887), *Sitzungsb. d. Berl. Akad.* (1895), 167, H. Weber, *Algebra* **2**, 23.)

Auch die Anzahl der Klassen konjugierter Elemente einer endlichen Gruppe $\mathfrak{G}$ der Ordnung g ist endlich. Zerfallen die Elemente von $\mathfrak{G}$ in k Klassen konjugierter Elemente, so mögen die einzelnen Klassen $\nu_1, \nu_2, \ldots, \nu_k$ verschiedene Elemente enthalten; dann ist $g = \nu_1 + \nu_2 + \cdots + \nu_k$. Sind die Zahlen $\nu_1, \nu_2, \ldots, \nu_k$ in der Folge $\nu_1 \leqq \nu_2 \leqq \cdots \leqq \nu_k$ geordnet, so ist $\nu_1 = 1$, da das Einheitselement als invariantes Element für sich allein eine Klasse bildet. Ist A_i ein Element der i^{ten} Klasse, so hat die Gruppe $\mathfrak{V}_i$, die aus den mit A_i vertauschbaren Elementen von $\mathfrak{G}$ besteht, die Ordnung $\frac{g}{\nu_i}$. Die Klasse der mit A_i ähnlichen Elemente besteht aus den ν_i Elementen: $A_i, G_2 A_i G_2^{-1}, G_3 A_i G_3^{-1}, \ldots G_{\nu_i} A_i G_{\nu_i}^{-1}$, wobei die Elemente $G_1 = 1, G_2, G_3, \ldots, G_{\nu_i}$ ein vollständiges Restsystem der Gruppe $\mathfrak{G}$ mod $\mathfrak{V}_i$ vorstellen. Mit Hilfe der angegebenen Resultate beweist man einen der wichtigsten Sätze der Theorie der endlichen Gruppen, nämlich den *Satz von Sylow* (*Math. Ann.* **5**, 586 (1872), eine Ableitung, die von Permutationen keinen Gebrauch macht, hat zuerst Frobenius, *Journ. f. Math.* **100**, 179 (1887) gegeben, ferner ebenda **101**, 282 (1887)):

Ist $\mathfrak{G}$ eine Gruppe der Ordnung g und die Zahl g durch die l^{te} Potenz der Primzahl p teilbar, so besitzt $\mathfrak{G}$ stets eine Untergruppe der Ordnung p^l.

In dem speziellen Fall $l = 1$ findet sich dieses Theorem bereits bei Cauchy in den *Exercices d'analyse* **3**, 250 (1844).

Ist p^m die *höchste* Potenz einer Primzahl p, die in g enthalten ist, so bezeichnet man die Untergruppen der Ordnung p^m einer Gruppe $\mathfrak{G}$ der Ordnung g als *Sylowsche Untergruppen* von $\mathfrak{G}$ (G. A. Miller, *Bull. Am. M. S.* (2) **9**, 543 (1903)).

Von seinen Untergruppen hat Sylow bewiesen: *Alle Sylowschen Untergruppen der Ordnung* p^m *einer Gruppe* $\mathfrak{G}$ *sind miteinander innerhalb* $\mathfrak{G}$ *ähnlich; ihre Anzahl* ϱ *ist eine Zahl der Form* $p\varrho' + 1$, *also kongruent* 1 (*mod* p). *Ist* $\mathfrak{S}$ *irgendeine Sylowsche Untergruppe von* $\mathfrak{G}$ *der Ordnung* p^m, *so hat* $\mathfrak{G}$ *die Ordnung* $p^m \cdot \varrho \cdot r$; *hierbei ist* r *nicht durch* p *teilbar und* $p^m \cdot r$ *die Ordnung der größten Untergruppe von* $\mathfrak{G}$, *deren Elemente mit der Gruppe* $\mathfrak{S}$ *vertauschbar sind.*

Jede Untergruppe von $\mathfrak{G}$ *der Ordnung* p^l *ist in einer der* ϱ *ähnlichen Sylowschen Untergruppen von* $\mathfrak{G}$ *der Ordnung* p^m *enthalten.*

Den von Sylow nur für die Anzahl ϱ der Sylowschen Untergruppen einer Gruppe $\mathfrak{G}$ bewiesenen Satz hat Frobenius (*Sitzungsb. d. Berl. Akad.* (1895), 981) dahin erweitert: *Die Anzahl der Untergruppen von* $\mathfrak{G}$ *der Ordnung* p^l, *wobei* g *auch durch eine höhere Potenz von* p *als die* l^{te} *teilbar sein kann, ist stets* $\equiv 1$ (*mod.* p). *Die Gruppen der Ordnung* p^l *sind, wenn* $l < m$ *ist, nicht notwendig miteinander ähnlich.*

Über die Sylowschen Sätze vgl. man noch Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), S. 170, sowie von Lehrbüchern: H. Weber, *Algebra* **2**, 135, W. Burnside, *Theory of groups*, S. 90, de Séguier, *Groupes abstraits*, S. 79, ferner G. A. Miller, *Bull. Am. M. S.* (2) **14**, 91 (1907), *Proc. Lond. M. S.* (2) **2**, 142 (1905).

Im Zusammenhang mit seiner Erweiterung des Sylowschen Satzes gelangte Frobenius (*Sitzungsb. d. Berl. Akad.* (1895), 981, ebenda (1903), 987) zu folgendem Fundamentalsatz über *die Potenzen eines Elementes einer endlichen Gruppe:*

Die Anzahl t *der Elemente* X *einer Gruppe* $\mathfrak{G}_g$, *deren* n^{te} *Potenz, also* X^n, *gleich einem beliebig vorgegebenen Element* A *von* $\mathfrak{G}$ *ist, ist durch den größten gemeinsamen Divisor* d *von* n *und* v *teilbar, wenn* v *die Anzahl der mit* A *vertauschbaren Gruppenelemente, also* $\frac{g}{v}$ *die Zahl der mit* A *ähnlichen Gruppenelemente von* $\mathfrak{G}$ *ist. Die Zahl* t *kann auch den Wert Null haben.*

Ist A ein *invariantes Element*, also im besonderen das Einheitselement E, so ist v gleich der Gruppenordnung g. Ist g durch n teilbar, so wird für ein invariantes Element die Zahl $d = n$. Die Gleichung $X^n = E$ wird stets durch $X = E$ befriedigt; daher ist für diesen Fall $t \neq 0$. Folglich ergibt sich:

Ist die Ordnung g *einer Gruppe* $\mathfrak{G}$ *durch die Zahl* n *teilbar, so ist die Anzahl* t *derjenigen Elemente der Gruppe* $\mathfrak{G}$, *deren*

Ordnung in n aufgeht, ein Vielfaches von n. Ist die Ordnung einer Gruppe 𝔊 durch n teilbar, so ist die von den t Elementen, welche der Gleichung $X^n = E$ genügen, erzeugte Gruppe entweder die Gruppe 𝔊 oder eine charakteristische Untergruppe von 𝔊, deren Ordnung ebenso wie die Zahl t durch n teilbar ist.

Von Lehrbüchern vgl. Burnside, *Theory of groups,* S. 110, de Séguier, *Groupes abstraits*, S. 74.

Anknüpfend an den Begriff der größten invarianten Untergruppe und die Sätze auf S. 188 erhält man für endliche Gruppen besonders bemerkenswerte Sätze: Ist 𝔊 eine endliche Gruppe, so heißt eine mit der Einheit endende Reihe von Gruppen: 𝔊, $\mathfrak{G}_1$, $\mathfrak{G}_2$, $\mathfrak{G}_3$, ..., 1, von denen jede Gruppe $\mathfrak{G}_i$ $(i = 1, 2, 3, \ldots)$ eine größte invariante Untergruppe der voraufgehenden $\mathfrak{G}_{i-1}$ ist, eine *Kompositionsreihe* oder eine *Reihe der Zusammensetzung der Gruppe* 𝔊. Für die Faktorgruppen $\mathfrak{G}/\mathfrak{G}_1$, $\mathfrak{G}_1/\mathfrak{G}_2$, $\mathfrak{G}_2/\mathfrak{G}_3$, ... beweist man: *Besitzt eine endliche Gruppe zwei verschiedene Kompositionsreihen, so sind, von der Reihenfolge abgesehen, die sich bei der einen Reihe ergebenden Faktorgruppen den aus der anderen Reihe entspringenden holoedrisch isomorph* (Hölder, *Math. Ann.* **34**, 37 (1889)). Sind g, g_1, g_2, ..., 1 die Ordnungen der Gruppen 𝔊, $\mathfrak{G}_1$, $\mathfrak{G}_2$, ..., 1, so heißen die Zahlen $\frac{g}{g_1} = e_1$, $\frac{g_1}{g_2} = e_2$, ... die *numerischen Faktoren der Zusammensetzung* oder die *Indexreihe der Gruppe* 𝔊. Als Ordnungen der Faktorgruppen $\mathfrak{G}/\mathfrak{G}_1$, $\mathfrak{G}_1/\mathfrak{G}_2$, ... sind, von der Reihenfolge abgesehen, die Zahlen e_1, e_2, ... *eindeutig* bestimmt (C. Jordan, *Traité*, p. 41). Neben der Reihe der Zusammensetzung kann man für eine endliche Gruppe 𝔊 auch eine *Hauptreihe* definieren (C. Jordan, *Traité*, p. 663). Die Gruppen: 𝔊, $\mathfrak{H}_1$, $\mathfrak{H}_2$, ..., 1 bilden eine Hauptreihe, wenn jede Gruppe $\mathfrak{H}_i$ $(i = 1, 2, 3, \ldots)$ nicht nur eine invariante Untergruppe der vorangehenden $\mathfrak{H}_{i-1}$ ($\mathfrak{H}_0 = \mathfrak{G}$), sondern sogar in der Gesamtgruppe 𝔊 invariant ist und zwischen zwei aufeinanderfolgenden Gruppen $\mathfrak{H}_{i-1}$ und $\mathfrak{H}_i$ es nie möglich ist, eine neue Gruppe einzuschieben, ohne daß die Reihe ihren Charakter verliert.

Wie auch immer die Hauptreihe 𝔊, $\mathfrak{H}_1$, $\mathfrak{H}_2$, .. 1 *einer endlichen abstrakten Gruppe gewählt sein mag, stets sind die Faktorgruppen* $\mathfrak{G}/\mathfrak{H}_1$, $\mathfrak{H}_1/\mathfrak{H}_2$, $\mathfrak{H}_2/\mathfrak{H}_3$, ... *bis auf die Reihenfolge dieselben, wenn man holoedrisch isomorphe Gruppen als nicht verschieden ansieht* (Hölder, *Math. Ann.* **34**, 38 (1889); daß die Zahlenfaktoren $\frac{g}{h_1}$, $\frac{h_1}{h_2}$, $\frac{h_2}{h_3}$, ..., abgesehen von der Reihenfolge, eindeutig bestimmt sind, bereits bei C. Jordan, a. a. O.). Jede

der aus einer Hauptreihe hervorgehenden Faktorgruppen $\mathfrak{G}/\mathfrak{H}_1$, $\mathfrak{H}_1/\mathfrak{H}_2$, $\mathfrak{H}_2/\mathfrak{H}_3$, ... ist eine elementare Gruppe (Hölder, a. a. O.). Eine Gruppe heißt nach Frobenius (*Sitzungsb. d. Berl. Akad.* (1902), 358) *elementar,* wenn sie einfach oder das direkte Produkt mehrerer holoedrisch isomorpher einfacher Gruppen ist. Das charakteristische Kennzeichen einer elementaren Gruppe ist, daß sie keine charakteristische Untergruppe besitzt.

Durch Einschieben von Gruppen kann man aus einer Hauptreihe eine Kompositionsreihe konstruieren, hingegen geht nicht stets durch Unterdrücken von Gruppen aus letzterer eine Hauptreihe hervor. Zu einer endlichen Gruppe $\mathfrak{G}$ kann man stets eine derartige Kompositionsreihe $\mathfrak{G}, \mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_i, \ldots, 1$ finden, daß, so oft sich die numerischen Faktoren der Zusammensetzung ändern, also $\frac{g_{i-1}}{g_i}$ von $\frac{g_i}{g_{i+1}}$ verschieden ist, $\mathfrak{G}_i$ eine invariante Untergruppe von $\mathfrak{G}$ ist (vgl. H. Weber, *Algebra* **2**, 33). Zu einer endlichen Gruppe läßt sich auch eine *lückenlose Reihe charakteristischer Untergruppen* konstruieren (Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 1027).

Ist g eine gegebene Zahl, so existiert nur eine endliche Anzahl nicht isomorpher abstrakter endlicher Gruppen, welche die Ordnung g besitzen. Man kann sich daher die Aufgabe stellen, alle nicht isomorphen abstrakten endlichen Gruppen der vorgegebenen Ordnung g mit Angabe ihrer definierenden Gleichungen aufzuzählen. Ist p eine Primzahl, so gibt es nur eine Gruppe p^{ter} Ordnung, nämlich die durch $A^p = 1$ definierte zyklische Gruppe. Nicht isomorphe Gruppen der Ordnung p^2 existieren nur 2, die beide Abelsche Gruppen sind; solche der Ordnung p^3 gibt es 3 Abelsche und 2 nicht Abelsche (Hölder, *Math. Ann.* **43**, 301 (1893)). Sind p und q voneinander verschiedene Primzahlen ($p > q$), so gibt es, wenn $p - 1$ nicht durch q teilbar ist, nur eine Gruppe der Ordnung pq, diese ist zyklisch. Im anderen Fall gibt es noch eine zweite Gruppe der Ordnung pq; diese wird durch $A_1^p = 1$, $A_2^q = 1$, $A_2^{q-1}A_1A_2A_1^{p-\alpha} = 1$ definiert, wobei α eine beliebige Zahl bedeutet, die mod p zum Exponenten q gehört (Netto, *Substitutionentheorie*, S. 134, Hölder, a. a. O., S. 312). Zusammenfassende Angaben über die verschiedenen Typen nicht isomorpher abstrakter endlicher Gruppen bei Easton, *The constructive development of group-theory,* S. 77, vgl. zur Ergänzung: G. A. Miller, *Bull. Am. M. S.* (2) **14**, 89 (1907).

Ist die Zahl k der Klassen konjugierter Elemente einer endlichen abstrakten Gruppe gegeben, so gibt es nur eine endliche Anzahl nicht isomorpher endlicher abstrakter Gruppen, welche die vorgegebene Klassenzahl k besitzen (Landau, *Math. Ann.* **56**, 674 (1903)).

Die Isomorphismengruppe einer endlichen Gruppe der Ordnung g ist höchstens von der Ordnung $(g-1)!$ und erreicht diesen Maximalwert nur für $g = 1, 2, 3$ und die nicht zyklische Gruppe der Ordnung 4. Eine Besprechung der Untersuchungen über die Isomorphismengruppe bei G. A. Miller, *Bull. Am. M.* S. (2) **14**, 124 (1907).

§ 4. Auflösbare, einfache und zusammengesetzte Gruppen.

Eine endliche Gruppe heißt auflösbar (C. Jordan), wenn ihre Indexreihe aus lauter Primzahlen besteht. H. Weber (*Algebra* **1**, 647) bezeichnet die auflösbaren Gruppen als *metazyklisch*.

Eine Gruppe ist dann und nur dann auflösbar, wenn die Ordnungen der Faktorgruppen, die irgendeine Hauptreihe der Gruppe liefert, Primzahlen oder ihre Potenzen sind.

Eine Gruppe ist dann und nur dann auflösbar, wenn für ihre sukzessiven Kommutatorgruppen folgendes eintritt: Bildet man die Kommutatorgruppe der Gruppe, von dieser wiederum die Kommutatorgruppe usw., so gelangt man schließlich zur Einheit (C. Jordan, *Traité*, S. 395; G. A. Miller, *Quart. J.* **28**, 268 (1896)).

Alle Gruppen der Ordnung p^m (p Primzahl) sind stets auflösbar (Sylow, *Math. Ann.* **5**, 588 (1872), Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 173 u. 982, W. Burnside, *Theory of groups*, Chap. V, de Séguier, *Groupes abstraits*, Chap. IV.)

Die Gruppen der Ordnung p^m und diejenigen, die das direkte Produkt von ihnen sind, erschöpfen sämtliche Gruppen, bei denen sich *jede* Untergruppe in eine der verschiedenen Kompositionsreihen, die man zu der gegebenen Gruppe konstruieren kann, einordnen läßt. Solche Gruppen heißen *spezielle Gruppen*. (W. Burnside, *Theory of groups*, S. 115, A. Loewy, *Math. Ann.* **55**, 67 (1902), de Séguier, *Groupes abstraits*, S. 87).

Satz von Frobenius (*Sitzungsb. d. Berl. Akad.* (1893), 342, (1895), 1043, Hölder, *Gött. Nachr.* (1895), 211, H. Weber, *Algebra* **2**, 140): *Jede Gruppe, deren Ordnung ein Produkt lauter verschiedener Primzahlen ist, ist auflösbar.*

Es gilt folgender allgemeiner Satz (Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 1041): *Ist* $\mathfrak{G}$ *eine Gruppe der Ordnung* $g = p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_n^{\lambda_n}$, *wobei* $p_1 < p_2 < \cdots < p_n$ *ihrer Größe nach geordnete Primzahlen bedeuten, und sind sämtliche in* $\mathfrak{G}$ *enthaltene Sylowsche Gruppen* $\mathfrak{P}_i$ *der Ordnungen* $p_i^{\lambda_i}$ $(i = 1, 2, \ldots, n-1)$ *ausnahmslos kommutative Gruppen vom Range* 1 *oder* 2 (vgl. S. 203), *so ist* $\mathfrak{G}$ *eine auflösbare Gruppe. Eine Ausnahme kann nur eintreten, wenn* $p_1 = 2$, $p_2 = 3$, $\mathfrak{P}_1$ *den Rang* 2 *hat und* $\mathfrak{G}$ *eine Untergruppe besitzt, deren Ordnung in* $2^{\lambda_1} 3^{\lambda_2}$ *aufgeht und mit der Tetraëdergruppe der Ordnung* 12 *isomorph ist.*

Haben die Exponenten $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ die Werte 1 oder 2, so sind die Gruppen $\mathfrak{P}_i$ $(i = 1, 2, \ldots, n-1)$ sicher kommutative Gruppen vom Range 1 oder 2. Mithin folgt: *Jede Gruppe der Ordnung* $p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_n^{\lambda_n}$, *bei der* $p_1 < p_2 < \cdots < p_n$ *ihrer Größe nach geordnete Primzahlen sind, jeder der Exponenten* $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ *den Wert* 1 *oder* 2 *besitzt,* λ_n *eine beliebige ganze positive Zahl bedeutet, ist auflösbar; eine Ausnahme kann nur* $p_1 = 2$, $p_2 = 3$, $\lambda_1 = 2$ *bilden.*

Satz von W. Burnside (*Proc. Lond. M. S.* (2) **1**, 388 (1904) u. (2) **2**, 432 (1905)): *Die Gruppen der Ordnung* $p^\alpha q^\beta$ (*p und q verschiedene Primzahlen*) *sind auflösbar.* (Spezialfälle sind früher von Frobenius, Burnside, Jordan behandelt worden, vgl. H. Weber, *Algebra* **2**, 145 und Frobenius, *Acta math.* **26**, 189 (1902), siehe auch Cole, *Trans. Am. M. S.* **5**, 214 (1904)). Der Beweis des Burnsideschen Satzes ergibt sich aus seinem (*Proc. Lond. M. S.* (2) **1**, 392) Theorem: *Jede endliche Gruppe, bei der die Anzahl von Elementen in einer Klasse konjugierter Elemente eine Primzahlpotenz ist, kann nicht einfach sein.*

Jede Gruppe, deren Ordnung das Produkt von drei Primzahlen ist, ist auflösbar. Über Gruppen, deren Ordnungen das Produkt von 4 und 5 Primzahlen sind, vgl. unten.

Jede Gruppe der Ordnung $p^4 q r$, *wobei* p, q, r *beliebige verschiedene ungerade Primzahlen bedeuten, ist auflösbar* (Burnside, *Proc. Lond. M. S.* **33**, 266 (1901), Frobenius, *Sitzungsb. d. Berl. Akad.* (1901), 1329).

Folgende Sätze von Frobenius erweisen eine Gruppe als zusammengesetzt:

Ist die Gruppe $\mathfrak{H}_h$ *in einer Gruppe* $\mathfrak{G}$ *der Ordnung hn enthalten und ist sie darin mit n verschiedenen Gruppen konjugiert, von denen je zwei teilerfremd sind, so enthält* $\mathfrak{G}$ *eine und nur eine, demnach charakteristische Untergruppe der Ordnung n* (*Sitzungsb. d. Berl. Akad.* (1901), 1226).

Enthält die Ordnung g einer Gruppe 𝔊 die Primzahl p in der ersten Potenz und ist p — 1 und g teilerfremd, so enthält 𝔊 eine und auch nur eine, demnach charakteristische Untergruppe der Ordnung $\frac{g}{p}$ (*Sitzungsb. d. Berl. Akad.* (1901), 849).

Verallgemeinerungen ebenda, vgl. ferner J. Schur, *Sitzungsb. d. Berl. Akad.* (1902), 1013.

Einfache, nicht isomorphe Gruppen, deren Ordnungen zusammengesetzt und kleiner als 2000 sind, gibt es nur sechs, nämlich je eine der Ordnungen: 60, 168, 360, 504, 660 und 1092 (Galois (1—60), *Œuvres*, p. 26, Hölder, *die einfachen Gruppen im ersten und zweiten Hundert der Ordnungszahlen*, *Math. Ann.* **40**, 55 (1892), Cole (200—600), *Am. J. math.* **14**, 378 (1892) und **15**, 303 (1893), W. Burnside (660—1092), *Proc. Lond. M.* S. **26**, 325 (1895), Ling and G. A. Miller (1092—2001), *Am. J. math.* **22**, 13 (1900)). Diese sechs Gruppen sind mit Gruppen des unendlichen Systems einfacher Gruppen holoedrisch isomorph, das die *verallgemeinerte endliche Modulargruppe* der Ordnung $\frac{p^m(p^{2m}-1)}{d}$ ($d = 1$ oder 2, je nachdem die Primzahl $p = 2$ oder größer als 2 ist) für die Werte $p^m = 5$ (oder 2^2), 7, 3^2, 2^3, 11, 13 (vgl. § 7) liefert. Die einfache Gruppe der Ordnung 60 wird durch zwei unabhängige Elemente S_1 und S_2 erzeugt; $S_1^5 = 1$, $S_2^2 = 1$, $(S_1 S_2)^3 = 1$ sind die Definitionsgleichungen der Gruppe.

Unter allen Gruppen, deren Ordnungen das Produkt von 4 *oder* 5 *Primzahlen sind, sind nur die vier Gruppen der Ordnungen* 60, 168, 660 *und* 1092 einfach (Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 1041, über Gruppen, deren Ordnungen das Produkt von 4 Primzahlen ist, vgl. auch Glenn, *Trans. Am. M. S.* **7**, 137 (1906)).

Ein Verzeichnis der bekannten einfachen Gruppen gibt Dickson, *Linear groups*, S. 309. In dieser Liste nicht aufgeführt ist das später bekannt gewordene unendliche System einfacher Gruppen der Ordnung $p^{6q}(p^{6q}-1)(p^{2q}-1)$, das für jede Primzahl $p > 2$ und jede ganze Zahl $q \geqq 1$ und für $p = 2$ und jedes ganzzahlige $q > 1$ existiert (Dickson, *Trans. Am. M. S.* **2**, 389 (1901), *Math. Ann.* **60**, 137 (1905)). Für jede Zahl der Form $\frac{1}{2}(p^{m(2r)}-1)\cdot p^{m(2r-1)}\cdot(p^{m(2r-2)}-1)$ $p^{m(2r-3)}\cdots(p^{2m}-1)\,p^m$, wobei p eine beliebige, von 2 verschiedene Primzahl, r und m beliebige ganze positive Zahlen,

$r > 2$ bedeuten, existieren sogar zwei einfache, nicht isomorphe Gruppen der angegebenen Ordnungszahl (Dickson, *Linear groups*, S. 309). Abgesehen von der abstrakten Gruppe der Ordnung $\frac{n!}{2}$, die mit der alternierenden Permutationsgruppe (vgl. § 6) isomorph ist, entstammen die bekannten Systeme einfacher Gruppen der Theorie der Kongruenzgruppen (vgl. § 12); die einfache Gruppe niedrigster Ordnung, die sich keinem System einordnen läßt, ist von der Ordnung 7920; sie läßt sich als vierfach transitive Permutationsgruppe des Grades 11 darstellen (Cole, *Quart. Journ.* **27**, 48 (1895), de Séguier, *Journ. de math.* (5) **8**, 291 (1902)). Die weiteren bekannten einfachen Gruppen, die sich bisher keinem System einordnen lassen, sind zwei Gruppen der Ordnungen 95040 und 244823040, die mit den zwei von Mathieu (*Journ. de math.* (2) **6**, 270 (1861), (2) **18**, 25 (1873)) entdeckten fünffach transitiven Permutationsgruppen der Grade 12 und 24 (W. Burnside, *Theory of groups*, 220, Frobenius, *Sitzungsb. d. Berl. Akad.* (1904), 567) holoedrisch isomorph sind, sowie zwei größte Untergruppen der letzten Gruppe, die als Permutationsgruppen der Grade 22 und 23 darstellbar sind (G. A. Miller, *Bull. de la soc. math.* **28**, 266 (1900)). Eine einfache Gruppe ungerader, zusammengesetzter Ordnung ist nicht bekannt. (Über den Stand dieser Frage vgl. Rietz, *Am. J. math.* **26**, 1 (1904).)

Nicht auflösbare abstrakte Gruppen, deren Ordnungen < 480 ist, gibt es nur die folgenden 25 nicht isomorphen:

Ordnung:	60	120	168	180	240	300	336	360	420
Anzahl:	1	3	1	1	8	1	3	6	1

(Hölder, *Math. Ann.* **46**, 420 (1895)).

§ 5. Abelsche Gruppen. Hamiltonsche Gruppen. Die Quaternionengruppe.

Jede Gruppe, die nur aus vertauschbaren Operationen besteht, heißt eine *Abelsche* oder *kommutative* Gruppe (vgl. S. 174). In jeder endlichen abstrakten Abelschen Gruppe $\mathfrak{G}$ kann man stets ein System erzeugender Elemente $A_1, A_2, \ldots, A_\sigma$ der Ordnungen $g_1, g_2, \ldots, g_\sigma$ derartig auswählen, daß das Produkt $g_1 g_2 \ldots g_\sigma$ gleich der Ordnung von $\mathfrak{G}$ ist und jedes Element von $\mathfrak{G}$ ein und auch nur einmal in der Form $A_1^{h_1} A_2^{h_2} \ldots A_\sigma^{h_\sigma}$ erscheint, wenn $h_1, h_2, \ldots, h_\sigma$ alle ganzzahligen Werte von 0 bis

$g_1 - 1$, bzw. 0 bis $g_2 - 1$ usw., 0 bis $g_\sigma - 1$ annehmen. Ein System von Elementen, das sich zu einer solchen Darstellung eignet, heißt eine *Basis der Abelschen Gruppe;* die erzeugenden Elemente der Basis heißen *Basiselemente.*

Eine Basis einer Abelschen Gruppe kann verschiedenartig gewählt werden; auch die Anzahl der Basiselemente ist nicht für jede Gruppe die gleiche. Bei jeder endlichen Abelschen lassen sich die Basiselemente derartig wählen, daß ihre Ordnungen Primzahlen oder ihre Potenzen sind. Die auf diese Weise gewonnenen Primzahlpotenzen heißen die *Invarianten der Gruppe.* Zwei Abelsche Gruppen sind dann und nur dann holoedrisch isomorph, wenn sie die gleichen Invarianten haben.

Eine Abelsche Gruppe von Primzahlpotenzordnung $p^m (m \geqq 1)$ mit den Invarianten $p^{\alpha_1}, p^{\alpha_2}, \ldots p^{\alpha_l}$ $(\alpha_1 + \alpha_2 + \cdots + \alpha_l = m)$ heißt vom *Typus* $(\alpha_1, \alpha_2, \ldots, \alpha_l)$. Da alle Abelschen Gruppen mit denselben Invarianten isomorph sind, existieren bei gegebenem p und m nur soviel verschiedene Abelsche Gruppen der Ordnung p^m, als es verschiedene additive Zerlegungen der Zahl m gibt.

Bei jeder endlichen Abelschen Gruppe kann man eine Basis auch derartig wählen, daß die Ordnungszahl jedes voraufgehenden Basiselementes A_i entweder durch die Ordnungszahl des folgenden A_{i+1} teilbar oder ihr gleich ist. Auf diese Weise erhält man die kleinste Anzahl von Basiselementen; diese kleinste Anzahl erzeugender Elemente der Abelschen Gruppe heißt der *Rang* der Abelschen Gruppe. Der Begriff der Invarianten wurde allerdings in anderer Fassung von Frobenius u. Stickelberger (*Journ. f. Math.* **86**, 236 (1879)) eingeführt; die obige Definition geht auf H. Weber zurück. Vgl. H. Weber, *Algebra* **2**, 38ff. Ist m eine beliebige ganze Zahl, so bilden die $\varphi(m)$ ganzen positiven Zahlen, die kleiner als m und relativ prim zu m sind, wenn man sie multiplikativ verknüpft und die sich bei der Multiplikation ergebenden Zahlen stets mod m nimmt, eine Abelsche Gruppe der Ordnung $\varphi(m)$.

Wegen unendlicher Abelscher Gruppen vgl. H. Weber, *Math. Ann.* **48**, 435 (1897) und de Séguier, *Groupes abstraits,* S. 97.

Jede endliche Gruppe, deren sämtliche Untergruppen invariant sind, heißt eine *Hamiltonsche Gruppe.* (Dedekind, *Math. Ann.* **48**, 548 (1897), G. A. Miller, *C. R.* **126**, 1406 (1898),

Bull. Am. M. S. (2) **4**, 510, (1898), E. Wendt, *Math. Ann.* **59**, 187 (1904), **60**, 319 (1905)). Eine besonders wichtige Hamiltonsche Gruppe ist die *Quaternionengruppe;* hierunter versteht man die Gruppe 8ter Ordnung, die durch die zwei unabhängigen Elemente i_1 und i_2 erzeugt wird und deren definierende Gleichungen: $i_1^4 = 1$, $i_1^2 i_2^2 = 1$, $i_1 i_2 i_1 i_2^3 = 1$ lauten. Für die Zusammensetzung der Quaternioneneinheiten (vgl. S. 16 und setze $i_1 i_2 = i_3$ und $i_1^2 = -1$) gelten genau die gleichen Kompositionsregeln wie für die Quaternionengruppe. Die Quaternionengruppe besitzt drei Untergruppen vierter und eine zweiter Ordnung.

Jede Hamiltonsche Gruppe, die keine Abelsche Gruppe ist, ist das direkte Produkt einer Quaternionengruppe, einer Abelschen Gruppe, deren sämtliche Elemente die Ordnung 2 haben, und einer Abelschen Gruppe ungerader Ordnungszahl. Umgekehrt ist jede derartige Gruppe eine Hamiltonsche Gruppe. Verallgemeinerungen der Hamiltonschen Gruppen: G. A. Miller, *Math. Ann.* **60**, 597 (1905), *Arch. f. Math.* (3) **11**, 76 (1906), Wendt, *Math. Ann.* **62**, 381 (1906).

Jede Untergruppe einer Abelschen Gruppe ist wiederum Abelsch. Es gibt auch nicht-Abelsche Gruppen, deren sämtliche Untergrupppen Abelsche Gruppen sind; ihre Ordnung ist nie durch mehr als zwei verschiedene Primzahlen teilbar (Miller and Moreno, *Trans. Am. M. S.* **4**, 398 (1903)). Eine Gruppe, deren Kommutatorgruppe nur aus invarianten Elementen besteht, heißt *metabelsch* (W. B. Fite, *Trans. Am. M. S.* **3**, 331 (1902)).

§ 6. Permutationen. Symmetrische und alternierende Gruppe.

Diejenige Operation, die n Symbole (man sagt auch Ziffern, Zahlen, Buchstaben, Marken) durch die gleichen Symbole in der nämlichen oder einer anderen Anordnung ersetzt, heißt eine *Permutation* oder *Substitution* (in engerem Sinn). Bezeichnet man die zu vertauschenden Symbole mit $1, 2, 3, \ldots, n$ und irgendeine Anordnung von ihnen mit $\alpha_1, \alpha_2, \ldots, \alpha_n$, so schreibt man die Permutation, die 1 durch α_1, 2 durch α_2, ..., n durch α_n ersetzt, $\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \end{pmatrix}$. (Cauchy, *Œuvres* (2) **1**, 67, manche Autoren schreiben umgekehrt nach Cauchys späteren Arbeiten, *Œuvres* (1) **9**, 281 $\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$.) Häufig

bezeichnet man eine Permutation abgekürzt mit einem einzigen Buchstaben A.

Jede Permutation kann auf $n!$ Arten geschrieben werden, indem man entweder den Zähler oder den Nenner beliebig anordnet und nur den Zusammenhang zwischen den übereinanderstehenden Symbolen nicht stört. Ist $a_1, a_2, \ldots, a_n$ irgendeine Anordnung der Zahlen $1, 2, \ldots, n$, so kann man die Permutation $A = \begin{pmatrix} 1 & 2 & 3 & \ldots n \\ \alpha_1 & \alpha_2 & \alpha_3 & \ldots \alpha_n \end{pmatrix}$ auch gleichwertig $\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ \alpha_{a_1} & \alpha_{a_2} & \ldots & \alpha_{a_n} \end{pmatrix}$ schreiben. Bei einer Permutation läßt man häufig die sich nicht ändernden Symbole fort.

Die Anzahl n der Symbole, auf die sich die Permutation bezieht, heißt der *Grad der Permutation*; die Anzahl der Symbole, die durch von ihnen verschiedene ersetzt werden, heißt die *Klasse der Permutation.*

Aus zwei Permutationen

$$A = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 1 & 2 & \ldots & n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \beta_{\alpha_1} & \beta_{\alpha_2} & \ldots & \beta_{\alpha_n} \end{pmatrix}$$

entspringt eine dritte

$$C = \begin{pmatrix} 1 & 2 & \ldots & n \\ \beta_{\alpha_1} & \beta_{\alpha_2} & \ldots & \beta_{\alpha_n} \end{pmatrix},$$

das *Produkt* von A und B. Man schreibt $C = AB$. (Manche Autoren bezeichnen umgekehrt das so gebildete Produkt C mit BA.)

Eine Permutation heißt *zyklisch* oder *zirkular*, wenn sich alle ihre Symbole oder bei Fortlassung der sich nicht ändernden die übrigen so anordnen lassen, daß das erste Symbol durch das zweite, das zweite durch das dritte, usw., das letzte durch das erste ersetzt wird. Eine zyklische Permutation hat bei Fortlassung der unverändert bleibenden Symbole die Form:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_{m-1} & \alpha_m \\ \alpha_2 & \alpha_3 & \ldots & \alpha_m & \alpha_1 \end{pmatrix} \quad (m \leqq n).$$

Man bezeichnet sie mit $(\alpha_1, \alpha_2, \ldots, \alpha_m)$, indem man die Symbole in der Reihenfolge, in der das eine für das andere tritt, in eine Klammer hintereinander setzt. Die zyklische Permutation läßt sich daher auf m Arten schreiben:

$$(\alpha_1, \alpha_2, \ldots, \alpha_m) = (\alpha_2, \alpha_3, \ldots, \alpha_m, \alpha_1) = \cdots = (\alpha_m, \alpha_1, \alpha_2, \ldots, \alpha_{m-1}).$$

Eine Permutation, bei der nur zwei Symbole vertauscht

werden, also eine zyklische Permutation (a, b), heißt eine *Transposition.*

Jede Permutation kann, abgesehen von der Reihenfolge, auf eine und auch nur auf eine Weise als ein Produkt zyklischer Permutationen, die kein Symbol gemeinsam haben, dargestellt werden. Diese zyklischen Faktoren heißen die *Zykeln der betr. Permutation.*

Eine zyklische Permutation oder eine solche, bei der jeder Zyklus, abgesehen von den eingliedrigen, die gleiche Anzahl von Symbolen enthält, heißt eine *reguläre Permutation.*

Jede Permutation n^{ten} Grades mit r Zykeln, wobei die eingliedrigen mitzurechnen sind, kann durch $n - r$ Transpositionen ersetzt werden. (Vgl. S. 44.) *Jede Permutation kann auf unendlich viele Weisen als Produkt von Transpositionen dargestellt werden; dabei ist sie entweder das Produkt einer stets geraden oder einer stets ungeraden Anzahl von Transpositionen.*

Eine Permutation heißt *gerade, von der ersten Klasse* oder *eigentlich*, wenn sie aus einer geraden Anzahl von Transpositionen gebildet werden kann; im anderen Fall heißt sie *ungerade*, von der *zweiten Klasse* oder *uneigentlich.*

Ist A eine gegebene Permutation n^{ten} Grades, so ist die Anzahl der Arten, auf die sich A als Produkt von w Transpositionen darstellen läßt, gleich

$$c_1 f_1^w + c_2 f_2^w + \cdots + c_k f_k^w;$$

hierbei hängen $f_1, f_2, \ldots, f_k$ nur von n allein ab und sind ganze Zahlen, $c_1, c_2, \ldots, c_k$ sind rationale, von n und der gegebenen Permutation, aber nicht von w abhängige Zahlen, die mit den Gruppencharakteren der symmetrischen Gruppe (vgl. § 10) in Zusammenhang stehen. (A. Hurwitz, *Math. Ann.* **39**, 7 (1891), **55**, 53 (1902), Netto, ebenda **56**, 482 (1903), Frobenius, *Sitzungsb. d. Berl. Akad.* (1903), 357.)

Die n! verschiedenen Permutationen von n Symbolen bilden bei ihrer Komposition eine endliche Gruppe, die symmetrische Gruppe der Ordnung n! (Der Name von C. Jordan, *Journ. de math.* (2) **16**, 383 (1871)).

Die für endliche Gruppen allgemein definierten Begriffe können für die symmetrische Gruppe verwendet werden. Ihre *Einheit*, die mit 1 bezeichnet wird, ist die *identische* Permutation $\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$, die alle Elemente ungeändert läßt. Die zu

$A = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \end{pmatrix}$ *reziproke* oder *inverse Permutation* lautet $A^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$. Die *Ordnung einer Permutation* ist die kleinste positive Zahl a, für die $A^a = 1$ wird.

Die Ordnung irgendeiner Permutation ist das kleinste gemeinsame Vielfache der Anzahl von Symbolen ihrer einzelnen Zykeln. Im besonderen ist die Ordnung einer regulären Permutation gleich der Anzahl von Symbolen irgendeines ihrer Zykeln.

Ist A irgendeine Permutation der Ordnung n und d der größte gemeinsame Teiler der positiven ganzen Zahlen x und n, so hat die Permutation A^x die Ordnung $\frac{n}{d}$; ist A zyklisch, so ist A^x regulär und zerfällt in d Zykeln von je $\frac{n}{d}$ Symbolen. Jede reguläre Permutation ist die Potenz einer zyklischen Permutation.

Auch eine geringere Anzahl als die Gesamtheit aller Permutationen der symmetrischen Gruppe der Ordnung $n!$ kann für sich eine Gruppe bilden. Jede solche Untergruppe der symmetrischen Gruppe heißt eine *Permutationsgruppe.* Die Anzahl der Elemente, auf die sich die Gruppe bezieht, heißt ihr *Grad,* die Anzahl der Permutationen, die sie enthält, ihre *Ordnung. Die Ordnung jeder Permutationsgruppe des Grades n ist ein Divisor von $n!$*

Enthält eine Permutationsgruppe eine Permutation der Klasse k und (abgesehen von der in jeder Gruppe vorhandenen Identität) keine von niedrigerer Klasse, so heißt die *Permutationsgruppe von der Klasse k.* (C. Jordan, *Journ. de math.* (2) **16**, 408 (1871)).

Alle geraden Permutationen von n Symbolen bilden eine Permutationsgruppe der Ordnung $\frac{n!}{2}$, die alternierende Gruppe.

Enthält eine Permutationsgruppe des Grades n die $n-2$ zyklischen Permutationen zweier fester Symbole mit den übrigen, also z. B. $(1, 2, 3), (1, 2, 4), \ldots (1, 2, n)$, *so ist sie entweder die alternierende oder die symmetrische Gruppe.*

Enthält eine Permutationsgruppe des Grades n die $n-1$ Transpositionen eines festen Symbols mit den übrigen, also z. B. $(1, 2), (1, 3), \ldots, (1, n)$, *so ist sie die symmetrische Gruppe.*

Die abstrakte Gruppe, die durch die $n-1$ unabhängigen Elemente $A_i (i = 1, 2, \ldots, n-1)$ mit den Gleichungen

$$A_1^2 = A_2^2 = \cdots = A_{n-1}^2 = 1,$$
$$A_i A_j = A_j A_i (i = 1, 2, \ldots, n-3;\ j = i+2,\ i+3, \ldots, n-1),$$
$$A_j A_{j+1} A_j = A_{j+1} A_j A_{j+1} (j = 1, 2, \ldots, n-2)$$

definiert wird, ist mit der symmetrischen Gruppe holoedrisch isomorph. Analoge Definition einer abstrakten Gruppe der Ordnung $\frac{n!}{2}$, die mit der alternierenden Gruppe des Grades n holoedrisch isomorph ist, durch $n-2$ unabhängige Elemente. (E. H. Moore, *Proc. Lond. M. S.* **28**, 357 (1897), Dickson, *Linear groups*, S. 287.)

Zwei Permutationen A und B von n Elementen heißen *konjugiert*, *ähnlich* oder *gleichberechtigt* — schärfer ausgedrückt: konjugiert in bezug auf die symmetrische Gruppe —, falls irgendeine Permutation C des nämlichen Grades existiert, daß $A = C^{-1}BC$ ist. *Zwei Permutationen sind dann und nur dann in bezug auf die symmetrische Gruppe konjugiert, falls sie gleichviele Zykeln mit gleichvielen Elementen besitzen.* Die Permutation $C^{-1}BC$ wird dadurch erhalten, daß man die Permutation C in den Zykeln der Permutation B ausführt. Teilt man die symmetrische Gruppe in k Klassen konjugierter Elemente, so umfaßt die ϱ^{te} Klasse $\frac{n!}{1^\alpha \cdot \alpha!\ 2^\beta \cdot \beta!\ 3^\gamma \cdot \gamma! \ldots}$ Permutationen, die aus α Zykeln mit einem Element, β Zykeln mit zwei Elementen, γ Zykeln mit drei Elementen, . . . bestehen. Die Anzahl k der Klassen konjugierter Elemente der symmetrischen Gruppe des Grades n ist gleich der Zahl der ganzzahligen positiven Lösungen $\alpha, \beta, \gamma, \ldots$ der Gleichung $n = \alpha + 2\beta + 3\gamma + \cdots$, wobei $\alpha, \beta, \gamma, \ldots$ auch Null sein können. (Cauchy, *Oeuvres* (1) **9**, 289).

Zwei Permutationen A und B, die einer Permutationsgruppe $\mathfrak{G}$ angehören, heißen *in bezug auf* $\mathfrak{G}$ *konjugiert*, *ähnlich* oder *gleichberechtigt*, falls in $\mathfrak{G}$ eine Permutation C existiert, daß $A = C^{-1}BC$ wird. Z. B. zwei Permutationen, die aus lauter Zykeln verschiedener ungerader Ordnungen bestehen und in bezug auf die symmetrische Gruppe ähnlich sind, brauchen es nicht in bezug auf die alternierende Gruppe zu sein. (Frobenius, *Sitzungsb. d. Berl. Akad.* (1901), 303.)

Zwei Permutationsgruppen $\mathfrak{H}_1$ und $\mathfrak{H}_2$ gleichen Grades

heißen *ähnlich, konjugiert*, auch *gleichberechtigt*, falls eine Permutation R des nämlichen Grades existiert, daß $\mathfrak{H}_2 = R\mathfrak{H}_1 R^{-1}$ wird. (Betrachtet man eine Permutationsgruppe als eine Gruppe linearer homogener Substitutionen, so kann man den Begriff der Ähnlichkeit zweier Permutationsgruppen weitergehend mittelst einer überführenden linearen homogenen Substitution definieren, ohne daß eine überführende Permutation zu existieren braucht. W. Burnside, *Proc. Lond. M. S.* **34**, 159 (1902).)

Ist $\mathfrak{H}$ eine Untergruppe der Permutationsgruppe $\mathfrak{G}$ und sind alle Permutationen G von $\mathfrak{G}$ mit $\mathfrak{H}$ vertauschbar, so ist $\mathfrak{H}$ eine *invariante Untergruppe* von $\mathfrak{G}$.

Die symmetrische Gruppe hat die alternierende Gruppe zur invarianten Untergruppe des Index 2.

Die alternierende Gruppe von mehr als vier Symbolen ist einfach (C. Jordan, *C. R.* **60**, 773 (1865), Kronecker, *Monatsb. d. Berl. Akad.* (1879), 208). Die alternierende Gruppe $\mathfrak{G}_{12}$ des Grades 4 besitzt eine invariante Untergruppe $\mathfrak{G}_4$ des Index 3; sie ist zugleich invariante Untergruppe der symmetrischen Gruppe $\mathfrak{G}_{24}$ und besteht aus der Identität und drei Paaren von Transpositionen (1, 2) (3, 4), (1, 3) (2, 4), (1, 4) (2, 3), von denen jede mit der Identität eine invariante Untergruppe von $\mathfrak{G}_4$ bildet. Die symmetrische Gruppe von 4, 3 und 2 Symbolen ist eine auflösbare Gruppe und besitzt die Indexreihe 2, 3, 2, 2 bezw. 2, 3 bezw. 2.

§ 7. Transitive, intransitive, primitive und imprimitive Permutationsgruppen. Reguläre Gruppen. Gruppen vom Primzahlgrad. Metazyklische Gruppe. Modulargruppe.

Eine Permutationsgruppe heißt *transitiv*, wenn ihre Permutationen irgendein Symbol in jedes überzuführen gestatten; eine transitive Permutationsgruppe besitzt Permutationen, die *jedes* Symbol in *jedes* überführen. Eine Permutationsgruppe n^{ten} Grades ist dann und nur dann transitiv, wenn sie n Permutationen der Form: $\begin{pmatrix}1 \dots \\ 1 \dots\end{pmatrix}, \begin{pmatrix}1 \dots \\ 2 \dots\end{pmatrix}, \begin{pmatrix}1 \dots \\ 3 \dots\end{pmatrix}, \dots \begin{pmatrix}1 \dots \\ n \dots\end{pmatrix}$ enthält.

Eine Permutationsgruppe heißt *intransitiv*, wenn die in ihr enthaltenen Permutationen wenigstens ein Symbol nicht in jedes beliebige überführen. Bei jeder intransitiven Gruppe $\mathfrak{G}$ können die Symbole so in m Teile *„Systeme der Intransitivität“*:

$$a_1, a_2, \dots;\ b_1, b_2, \dots;\ c_1, c_2, \dots;\ \dots;\ m_1, m_2, \dots,$$

zerlegt werden, daß die Permutationen der Gruppe die Symbole jedes Teiles transitiv untereinander vertauschen und nicht in diejenigen eines anderen überführen. Jede Permutation einer intransitiven Gruppe ist das Produkt $P_1 P_2 \ldots P_m$ von Permutationen $P_i (i = 1, 2, \ldots, m)$, von denen jede nur die Symbole aus einem System enthält. Die Permutationen P_i, die nur die Symbole des i^{ten} Systems der Intransitivität enthalten, bilden eine transitive Permutationsgruppe $\mathfrak{P}_i$. Die Permutationsgruppen $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_m$ heißen die *transitiven Komponenten* (Konstituenten) von $\mathfrak{G}$. Über intransitive Permutationsgruppen vgl. Bolza, *Am. J. math.* **11**, 195 (1889), Burnside, *Theory of groups,* S. 159.

Lassen sich die Symbole einer transitiven Permutationsgruppe des Grades n in m Systeme von je $\frac{n}{m}$ Symbolen verteilen, so daß die Permutationen der Gruppe die Symbole eines Systems entweder nur durcheinander oder durch sämtliche eines anderen Systems ersetzen, so heißt die Gruppe *imprimitiv*. Die m Systeme werden *Systeme der Imprimitivität* genannt. Eine transitive Gruppe, deren Symbole sich nicht so einteilen lassen, heißt *primitiv*.

Die Einteilung der Permutationsgruppen in die drei Klassen: intransitive, imprimitive und primitive geht auf Ruffini zurück.

Ist $\mathfrak{G}$ eine transitive Permutationsgruppe des Grades n und bilden die Permutationen von $\mathfrak{G}$, die ein bestimmtes Symbol ungeändert lassen, eine Gruppe $\mathfrak{H}$, so ist $\mathfrak{G}$ imprimitiv, wenn eine von $\mathfrak{G}$ und $\mathfrak{H}$ verschiedene Permutationsgruppe $\mathfrak{M}$ existiert, die $\mathfrak{H}$ enthält und in $\mathfrak{G}$ enthalten ist. Existiert kein solches $\mathfrak{M}$, so ist $\mathfrak{H}$ primitiv. (Dyck, *Math. Ann.* **22**, 94 (1883), Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 179.)

Jede invariante Untergruppe einer primitiven Permutationsgruppe ist transitiv. (Satz von Jordan, *Traité*, 41.) *Die Ordnung einer auflösbaren primitiven Permutationsgruppe ist eine Primzahlpotenz.* (Galois, *Œuvres,* p. 11.)

Besitzt eine imprimitive Permutationsgruppe eine invariante intransitive Untergruppe, so sind ihre Systeme der Intransitivität Systeme der Imprimitivität der gegebenen Gruppe. Besitzt eine imprimitive Gruppe $\mathfrak{G}$ m Systeme der Imprimitivität, so werden diese durch die Permutationen von $\mathfrak{G}$ nach einer transitiven Gruppe $\mathfrak{G}_1$ des Grades m permutiert, die mit der Faktorgruppe $\mathfrak{G}/\mathfrak{J}$ holoedrisch isomorph ist. Die invariante Untergruppe $\mathfrak{J}$ von $\mathfrak{G}$, die der Identität von $\mathfrak{G}_1$ entspricht, ist intransitiv und läßt die

m Systeme ungeändert. Die Gruppe $\mathfrak{J}$ kann auch unter Umständen die Identität sein.

Bei einer imprimitiven Permutationsgruppe können sich die Symbole verschiedenartig in Systeme der Imprimitivität zerlegen lassen (vgl. über imprimitive Gruppen die mit zahlreichen Literaturangaben versehene Arbeit von Kuhn, *Am. J. math.* **26**, 45 (1904)).

Die transitiven Permutationsgruppen werden in *einfach* und *mehrfach transitive* unterschieden. (Mathieu, *Journ. de math.* (2) **5**, 13 (1860).) Eine Permutationsgruppe heißt *k-fach transitiv*, wenn ihre Permutationen irgend k fest gewählte Symbole in k beliebige andere überzuführen gestatten. Eine k-fach transitive Gruppe besitzt eine Permutation, die *k beliebig ausgewählte* Symbole in *k beliebige* andere überführt. *Eine mehrfach transitive Gruppe ist stets primitiv.*

Die Ordnung einer k-fach $(k \geqq 1)$ *transitiven Permutationsgruppe vom Grade n ist gleich* $n(n-1)(n-2)\ldots(n-k+1)m$, *worin m die Ordnung einer Untergruppe bedeutet, deren Permutationen k beliebig ausgewählte Symbole ungeändert lassen.*

Ist die Gruppe $(n-k)^{ten}$ *Grades, die von allen denjenigen Permutationen einer wenigstens k-fach transitiven Permutationsgruppe* n^{ten} *Grades gebildet wird, die k bestimmte Symbole ungeändert lassen, noch* μ*-fach transitiv, so ist die Gruppe* n^{ten} *Grades* $(\mu+k)$*-fach transitiv.* (Frobenius, *Journ. f. Math.* **101**, 290 (1887).)

Eine Permutationsgruppe des Grades n, die nicht die alternierende Gruppe ihres Grades enthält, kann nicht mehr als $\left(\frac{n}{3}+1\right)$*-fach transitiv sein*[1], *die alternierende Gruppe ist* $(n-2)$*-fach, die symmetrische Gruppe n-fach transitiv.*

Enthält eine k-fach transitive Permutationsgruppe nicht die alternierende Gruppe ihres Grades, so ist ihre Klasse (vgl. S. 207) $> 2k-3$. *Besitzt also eine k-fach transitive Permutationsgruppe, abgesehen von der Identität, Permutationen, die weniger als* $2k-2$ *Symbole vertauschen, so ist sie die alternierende oder symmetrische Gruppe.*

Enthält eine k-fach transitive Permutationsgruppe des Grades n nicht die alternierende Gruppe ihres Grades, so ist ihre Klasse $> \frac{1}{4}n-1$, *wenn* $k>1$, $> \frac{1}{3}n-1$, *wenn* $k>2$ *und* $\geqq \frac{1}{2}n-1$,

1) Für die fünffach transitive Mathieusche Permutationsgruppe des Grades 12 (vgl. S. 202) wird dieses Maximum erreicht.

wenn $k > 3$. (Bochert, *Math. Ann.* **40**, 179 (1892); engere Grenzen: *Math. Ann.* **49**, 133 (1897), C. Jordan, *Journ. de math.* (5) **1**, 35 (1895), Maillet, *Mém. prés. par divers savants à l'acad. des sciences* **32**, (1902)).

In jeder transitiven Permutationsgruppe des Grades n gibt es wenigstens $n-1$ Permutationen, die alle Symbole vertauschen. Eine transitive Permutationsgruppe, bei der die Ordnung gleich dem Grade n ist, heißt *regulär. Eine solche enthält, abgesehen von der Identität, nur Permutationen, die alle Symbole vertauschen; sie läßt sich auch als eine transitive Permutationsgruppe des Grades und der Klasse n charakterisieren. Jede reguläre Gruppe, deren Grad eine zusammengesetzte Zahl ist, ist imprimitiv.*

Zu jeder regulären Permutationsgruppe des Grades n existiert eine mit ihr holoedrisch isomorphe derselben Symbole, sie umfaßt alle Permutationen und auch keine anderen als diejenigen, die mit jeder Permutation der ersten Gruppe vertauschbar sind. Der Durchschnitt der zwei Gruppen ist die Zentrale jeder von beiden.

Bei einer transitiven Permutationsgruppe $\mathfrak{G}$ des Grades n und der Klasse $n-1$ bilden die $n-1$ Permutationen, die alle Symbole umsetzen, zusammen mit der identischen Permutation eine charakteristische Untergruppe. Eine derartige Gruppe $\mathfrak{G}$ kann nur dann primitiv sein, wenn n eine Potenz einer Primzahl und die in $\mathfrak{G}$ enthaltene Untergruppe $\mathfrak{N}$ der Ordnung n eine elementare ist. Unter diesen Bedingungen ist $\mathfrak{G}$ stets dann und nur dann primitiv, wenn $\mathfrak{N}$ eine minimale invariante Untergruppe von $\mathfrak{G}$ ist. (Frobenius, *Sitzungsb. d. Berl. Akad.* (1901), 1226, (1902), 458.)

Eine Permutationsgruppe des Grades $r+k$, die nicht die alternierende Gruppe ihres Grades enthält, kann, wenn r irgendeine Primzahl ist, für $k > 2$ nicht mehr als k-fach transitiv sein. (C. Jordan, *Bull. de la soc. math.* **1**, 41, G. A. Miller, *Bull. Am. M. S.* **4**, 142 (1898).)

Für *transitive Permutationsgruppen vom Primzahlgrade p* gelten folgende Sätze:

Eine transitive Permutationsgruppe vom Primzahlgrad ist stets primitiv.

Ist der Grad einer transitiven Permutationsgruppe $\mathfrak{G}$ eine Primzahl p, so ist ihre Ordnung $= pq(\lambda p + 1)$, wo q ein Teiler von $p-1$ ist und $\lambda p + 1$ die Anzahl der verschiedenen in $\mathfrak{G}$ enthaltenen Untergruppen $\mathfrak{P}$ der Ordnung p bedeutet; diese Untergruppen sind sämtlich konjugiert. Alle mit einer beliebigen derartigen Gruppe $\mathfrak{P}$ vertauschbaren Elemente von $\mathfrak{G}$ bilden eine

Untergruppe der Ordnung pq von $\mathfrak{G}$. (Mathieu, *Journ. de math.* (2) **6**, 304 (1861).)

Enthält eine transitive Permutationsgruppe $\mathfrak{G}$ *vom Primzahlgrade* p *irgendeine invariante Untergruppe* $\mathfrak{J}$, *so ist* $\mathfrak{G}/\mathfrak{J}$ *eine zyklische Gruppe.* (G. A. Miller, *Bull. Am. M. S.* **4**, 141 (1898).)

Die Permutationen

$$\begin{pmatrix} 0 & 1 & 2 & \ldots & p-1 \\ \alpha & \alpha+\beta & \alpha+2\beta & \ldots & \alpha+(p-1)\beta \end{pmatrix},$$

wobei $\alpha = 0, 1, 2, \ldots, p-1$, $\beta = 1, 2, \ldots, p-1$ und die im Nenner der Permutation stehenden Zahlen immer durch ihre kleinsten Reste mod p zu ersetzen sind, bilden eine *Permutationsgruppe des Grades p und der Ordnung $p(p-1)$. Sie ist zweifach transitiv und auflösbar. Jede auflösbare transitive Permutationsgruppe vom Primzahlgrad p ist entweder diese Gruppe oder eine ihrer Untergruppen.* (Galois, *Œuvres*, p. 47.) Die fragliche Gruppe der Ordnung $p(p-1)$ heißt nach Kronecker (*Monatsb. d. Berl. Akad.* (1879), 217) *metazyklisch*, bei H. Weber, *Algebra* **1**, 666 die *volle lineare Gruppe*. Man stellt ihre Permutationen *„analytisch"* dar durch die Relation $|z, \alpha z + \beta|$, welche, wenn z die Werte $0, 1, 2, \ldots, p-1$ durchläuft, die Verknüpfung der im Zähler der Permutation stehenden Symbole mit den unter ihnen befindlichen des Nenners angibt. Die Gruppe wird erzeugt durch die zwei Permutationen $|z, z+1|$ und $|z, gz|$, wobei g eine primitive Wurzel der Primzahl p ist. Verallgemeinerung dieser Gruppe zu einer zweifach transitiven Permutationsgruppe des Grades p^m und der Ordnung $p^m(p^m-1)$ mit p^m konjugierten zyklischen Untergruppen der Ordnung $p^m - 1$, indem für die Primzahl p die p^m Zahlen des $GF[p^m]$ treten. Mathieu, *Journ. de math.* (2) **5**, 39 (1860), (2) **6**, 262 (1861) (eine weitere Verallgemeinerung), Burnside, *Theory of groups,* S. 155, de Séguier, *Journ. de math.* (5) **8**, 263 (1902).

Jede transitive Permutationsgruppe vom Primzahlgrade p ist entweder in der metazyklischen Gruppe enthalten oder wenigstens zweifach transitiv. W. Burnside, *Proc. Lond. M. S.* **33**, 163 (1901), *Quart. J.* **37**, 215 (1906), J. Schur, *Math. Ver.* **17**, 171 (1908).

Die metazyklische Gruppe und ihre Untergruppen, deren es für jeden Divisor q von $p-1$ eine gibt, sind die einzigen transitiven Permutationsgruppen vom Primzahlgrad p mit einer einzigen Untergruppe ($\lambda = 0$) *der Ordnung p.* Die Zahl λ muß

immer Null sein, wenn $q = 1$ ist oder, wenn für $q = 2$, die Primzahl p von der Form $4t + 3$ ist.

Für $\lambda = 1$ gilt der Satz:

Es gibt nur vier transitive Permutationsgruppen, deren Grad eine Primzahl p ist und die $p + 1$ Untergruppen der Ordnung p enthalten, die alternierende und die symmetrische Gruppe des Grades 5, *deren Ordnungen gleich* 60 *und* 120 *sind, und die beiden einfachen Gruppen der Grade* 7 *und* 11, *deren Ordnungen gleich* 168 *und* 660 *sind.* (Sylow, *Videnskabsselskabets Skrifter* I (1897), Frobenius, *Sitzungsb. d. Berl. Akad.* (1902), 352.)

Die Permutationen in $p + 1$ Symbolen, die mit $0, 1, 2, \ldots, p - 1, \infty$ bezeichnet seien,

$$\begin{pmatrix} 0 & 1 & 2 & 3 & \ldots & p-1 & \infty \\ \frac{\beta}{\delta} & \frac{\alpha+\beta}{\gamma+\delta} & \frac{2\alpha+\beta}{2\gamma+\delta} & \frac{3\alpha+\beta}{3\gamma+\delta} & \ldots & \frac{(p-1)\alpha+\beta}{(p-1)\gamma+\delta} & \frac{\alpha}{\gamma} \end{pmatrix}$$

bilden, wenn p eine ungerade Primzahl, $\alpha, \beta, \gamma, \delta$ beliebige Zahlen aus der Reihe $0, 1, 2, \ldots, p - 1$ sind, deren Determinante $\alpha\delta - \beta\gamma \neq 0$ ist, und die im Nenner der Permutation stehenden Zahlen mod p genommen werden, eine Gruppe; hierbei ist unter $\frac{a}{b}$ in üblicher Weise die Zahl x zu verstehen, die durch $bx \equiv a \pmod p$ bestimmt wird, und für $b = 0$, $a \neq 0$ ist $\frac{a}{b} = \infty$ zu setzen.

Die definierte Permutationsgruppe des Grades $p + 1$ hat die Ordnung $p(p^2 - 1)$ und ist dreifach transitiv. Ihre Permutationen werden „analytisch" dargestellt durch die Relation $\left| z, \frac{\alpha z + \beta}{\gamma z + \delta} \right|$, $\alpha\delta - \beta\gamma \neq 0$; diese gibt, wenn z die Werte $0, 1, 2, \ldots, p - 1, \infty$ durchläuft, die Verknüpfung der im Zähler der Permutation stehenden Symbole mit den unter ihnen befindlichen des Nenners an. *Die Gruppe der Ordnung $p(p^2 - 1)$ hat eine invariante, zweifach transitive Untergruppe des Grades $p + 1$ und der Ordnung $\frac{1}{2}p(p^2 - 1)$.* Ihre Permutationen werden definiert durch $\left| z, \frac{\alpha z + \beta}{\gamma z + \delta} \right|$ mit der Bedingung $\alpha\delta - \beta\gamma \equiv 1 \pmod p$. *Die Gruppe der Ordnung $\frac{1}{2}p(p^2 - 1)$ ist für $p > 3$ einfach.* Die letztere Gruppe ergibt sich als Galoissche Gruppe bei den Transformationsgleichungen der elliptischen Funktionen (Modulargleichungen) und heißt daher die *Modulargruppe.* Sie ist bereits von Galois,

Œuvres, p. 28, behandelt. Die Bestimmung der Untergruppen der Modulargruppe bei Gierster, *Math. Ann.* **18**, 319 (1881), vgl. Klein-Fricke, *Modularfunktionen* **1**, 411, Weber, *Algebra* **3**, 284.

Ist p eine Primzahl, so gibt es nicht mehr als eine transitive Gruppe des Grades $p+1$ und der Ordnung $\frac{1}{2}p(p^2-1)$; nur für $p=7$ gibt es zwei solche. Es gibt nicht mehr als eine transitive Gruppe des Grades $p+1$ und der Ordnung $p(p^2-1)$. (Frobenius, *Sitzungsb. d. Berl. Akad.* (1902), 353, 359.)

Die durch die Permutationen $\left| z, \frac{\alpha z+\beta}{\gamma z+\delta} \right|$ $(\alpha\delta-\beta\gamma \neq 0)$ definierte Gruppe des Grades $p+1$ läßt sich zu einer *dreifach transitiven Permutationsgruppe L des Grades p^m+1 und der Ordnung $p^m(p^{2m}-1)$* verallgemeinern, indem man sich statt der Primzahl p des Galoisschen Feldes $GF[p^m]$ bedient. Als die p^m+1 zu vertauschenden Symbole hat man die mit 0, 1, 2, ..., p^m-1 numerierten Zahlen des $GF[p^m]$ unter Zufügung des Symbols ∞ zu verstehen, $\alpha, \beta, \gamma, \delta$ durchlaufen die Zahlen des $GF[p^m]$, unter $\frac{a}{b}$ sei die durch $b\xi=a$ definierte Zahl ξ des $GF[p^m]$ verstanden. Ist $p=2$, so ist die Gruppe L mit der Gruppe L_0 der Permutationen $\left| z \ \frac{\alpha z+\beta}{\gamma z+\delta} \right|$, $\alpha\delta-\beta\gamma=+1$ identisch. Für $p>2$ hat die Gruppe L die Gruppe L_0 des Grades p^m+1 und der Ordnung $\frac{p^m(p^{2m}-1)}{2}$, die durch die Permutationen $\left| z \ \frac{\alpha z+\beta}{\gamma z+\delta} \right|$, $\alpha\delta-\beta\gamma=+1$ definiert wird und zweifach transitiv ist, zur invarianten Untergruppe. Die Permutationsgruppe L_0 des Grades p^m+1 und der Ordnung $\frac{p^m(p^{2m}-1)}{2}$ bezw. $2^m(2^{2m}-1)$ heißt die *verallgemeinerte endliche Modulargruppe.* (Mathieu, *Journ. de math.* (2) **5**, 39 (1860), E. H. Moore, *Math. papers of the Chicago Congress* (1893), publ. 1896, S. 208, *The decennial publications of the university of Chicago,* Vol. IX (1903), W. Burnside, *Proc. Lond. M. S.* **25** 113 (1894), Wiman, *Stockholm Akad. Bihang* **25** (1899), J. Schur, *Journ. f. Math.* **132**, 113 (1907), Dickson, *Linear groups,* S. 260, H. Weber, *Algebra* **2**, 310.) *Die verallgemeinerte Modulargruppe ist, abgesehen von den zwei Fällen $p^m=2$ und $p^m=3$, eine einfache Gruppe. Sie hat stets Untergruppen des Index p^m+1, aber nur für $p^m=2, 3, 5, 7, 3^2, 11$ solche von niederem Index, nämlich vom Index* 2, 3, 5, 7, 6, 11. (Für $m=1$ bereits

bei Galois, *Œuvres,* p. 29.) Außer für $p^m = 5, 7, 9, 11$ ist die verallgemeinerte Modulargruppe mit keiner Permutatiosgruppe niedrigeren Grades als mit einer des Grades $p^m + 1$ holoedrisch isomorph. In den Ausnahmefällen, wo ihre Ordnung 60, 168, 360 und 660 ist, kann sie auch als Permutationsgruppe in 5, 7, 6 und 11 Symbolen dargestellt werden und ist dann 3-, 2-, 4- und 2-fach transitiv.

Die Gruppe L der Ordnung $p^m(p^{2m} - 1)$ hat die oben S. 213 behandelte verallgemeinerte metazyklische Gruppe $|z, \alpha z + \beta|$ der Ordnung $p^m(p^m - 1)$ zur Untergruppe. (G. A. Miller, *Quart. J.* **34**, 232 (1903).)

§ 8. Permutationsgruppen höchster Ordnung bei gegebenem Grad. Die zu den Permutationsgruppen zugehörigen Funktionen. Die symmetrischen und alternierenden Funktionen.

Die Ordnung einer Permutationsgruppe n^{ten} Grades ist stets ein Teiler von $n!$, jedoch kann nicht jeder Teiler von $n!$ die Ordnung einer Permutationsgruppe n^{ten} Grades sein.

Die Aufgabe, Untergruppen der symmetrischen Gruppe von möglichst kleinem Index zu bestimmen, wird als *Bertrandsches Problem* (Bertrand, *J. éc. polyt. Cah.* **30**, 123 (1845)) bezeichnet. *Der Index einer intransitiven Untergruppe der symmetrischen Gruppe n^{ten} Grades ist gleich oder größer als n und nur dann gleich n, wenn die Permutationsgruppe ein Symbol fest läßt und die übrigen $n - 1$ Symbole auf alle $(n - 1)!$ Arten permutiert. Der Index einer imprimitiven Untergruppe der symmetrischen Gruppe von n Symbolen ist immer größer als n, abgesehen von $n = 4$. Für $n = 4$ existieren drei ähnliche imprimitive Gruppen 8ten Grades, also vom Index 3, von denen eine durch die zwei Permutationen $(12)(3)(4)$, $(13)(24)$ erzeugt wird. Ausgenommen für $n = 6$ gibt es keine primitive Permutationsgruppe in n Symbolen, deren Ordnung $\geqq (n - 1)!$ ist. Für $n = 6$ gibt es primitive Permutationsgruppen des Index 6, also von der Ordnung 120; eine solche wird durch die auf S. 214 besprochene der Primzahl $p = 5$ entsprechende Gruppe $(p + 1)^{\text{ten}}$ Grades der Ordnung $p(p^2 - 1)$ geliefert.* (Vgl. J. A. Serret, *Journ. de math.* **15**, 1 (1850), *Algèbre supérieure* **2**, 287, C. Jordan, *Traité,* 67, H. Weber, *Algebra* **2**, 154.)

Eine Aufzählung aller Permutationsgruppen einschließlich der intransitiven, deren Ermittlung sich stets auf transitive niedrigeren Grades zurückführen läßt, ist bis zum Grade $n = 11$ geleistet; bei den imprimitiven Permutationsgruppen ist man

bis zum Grade $n = 15$, bei den primitiven[1]) bis $n = 18$ gegangen. Literatur in der nicht abgeschlossenen Arbeit von E. N. Martin, *Am. J. math.* **23**, 285 (1901). Zur Ergänzung: Miller and Ling, *Quart. J.* **32**, 342 (1901), Kuhn, *Am. J. math.* **26**, 45 (1904). Vgl. auch die Zusammenstellung bei Easton, *The constructive development of group-theory,* p. 77.

Hat man eine rationale Funktion $\varphi(x_1, x_2, \ldots, x_n)$ der n Variablen $x_1, x_2, \ldots, x_n$ und führt auf sie sämtliche $n!$ Permutationen der n Zahlen $1, 2, \ldots, n$ aus, so bildet die Gesamtheit aller Permutationen, bei denen sich die Funktion φ nicht ändert, eine Permutationsgruppe $\mathfrak{G}$ n^{ten} Grades; sie heißt die *Gruppe der Funktion. Umgekehrt gehören zu jeder Permutationsgruppe* $\mathfrak{G}$ n^{ten} *Grades in den Zahlen* $1, 2, \ldots, n$ *eine und sogar unendlich viele rationale Funktionen der* n *Variablen* $x_1, x_2, \ldots, x_n$, *die nur bei den Permutationen aus* $\mathfrak{G}$ *und keinen anderen ungeändert bleiben.*

Eine rationale Funktion $\varphi(x_1, x_2, \ldots, x_n)$, die bei den Permutationen der symmetrischen Gruppe $\mathfrak{S}$ ϱ verschiedene Werte annimmt, heißt ϱ-*wertig*. Ist $\mathfrak{G}$ die Gruppe der Funktion φ, hat $\mathfrak{G}$ die Ordnung g und geht φ durch die Permutationen von $\mathfrak{S}$ in die ϱ verschiedenen Werte $\varphi_1 = \varphi, \varphi_2, \varphi_3, \ldots, \varphi_\varrho$ über, so ist $\varrho = \frac{n!}{g}$, *also gleich dem Index der Untergruppe* $\mathfrak{G}$ *von* $\mathfrak{S}$. (Lagrange.) Die ϱ Funktionen $\varphi_1, \varphi_2, \ldots, \varphi_\varrho$ heißen ein *System* (in bezug auf $\mathfrak{S}$) *konjugierter Funktionen.*

Jede Permutation aus $\mathfrak{S}$ permutiert die ϱ Funktionen untereinander. Geht φ_a $(a = 1, 2, \ldots, \varrho)$ durch eine Permutation A von $\mathfrak{S}$ in φ_b über und ist $\mathfrak{G}_1$ die Gruppe der Funktion φ_a, so geht φ_a nur durch die Permutationen der Nebengruppe $\mathfrak{G}_1 A$ in φ_b über und $A^{-1}\mathfrak{G}_1 A$ ist die zu φ_b gehörige Gruppe. *Zu konjugierten Funktionen gehören innerhalb* $\mathfrak{S}$ *ähnliche Permutationsgruppen.*

Da, abgesehen von $n = 4$, die symmetrische Gruppe außer der alternierenden Gruppe des Index 2 keine invariante Untergruppe besitzt, haben für $\varrho > 2$, abgesehen von $n = 4$, die zu einem System ϱ konjugierter Funktionen zugehörigen Permutations-

1) Primitive Permutationsgruppen ungerader Ordnung, deren Grad < 243 ist, existieren, abgesehen von Untergruppen der metazyklischen Gruppe, nur 10 der Ordnungen: 25. 3, 27. 13, 27. 39, 81. 5, 121. 3, 121. 15, 125. 31, 125. 93, 169. 7, 169. 21. Der erste Faktor gibt hierbei den Grad der betr. Permutationsgruppe an. H. L. Rietz, *Am. J. math.* **26**, 30 (1904).

gruppen keine andere gemeinschaftliche Permutation als die Einheit.

Abgesehen von $n = 4$, ist eine weniger als n-wertige Funktion von n Variablen 1- oder 2-wertig. (Folge des oben besprochenen Bertrandschen Problems.)

Für $n = 4$ gibt es dreiwertige Funktionen, nämlich das System konjugierter Funktionen:

$$\varphi_1 = \{(x_1 + x_2) - (x_3 + x_4)\}^2, \quad \varphi_2 = \{(x_1 + x_3) - (x_2 + x_4)\}^2,$$
$$\varphi_3 = \{(x_1 + x_4) - (x_2 + x_3)\}^2.$$

Die drei zu diesen Funktionen zugehörigen ähnlichen $\mathfrak{G}_8$ haben die in der symmetrischen Gruppe $\mathfrak{G}_{24}$ vierten Grades vorhandene invariante $\mathfrak{G}_4$ (vgl. S. 209) gemeinsam. Hierauf beruht Lagranges Auflösung der Gleichung vierten Grades (Lagrange, *Œuvres* **3**, 266, vgl. das Kapitel über Algebra § 8).

Die einwertigen rationalen Funktionen von n Größen heißen *symmetrisch. Jede rationale symmetrische Funktion ist der Quotient zweier ganzer rationaler symmetrischer Funktionen.*

Unter der symmetrischen Funktion $\sum x_1^{\nu_1} x_2^{\nu_2} \dots x_n^{\nu_n}$ ist der Gliederkomplex zu verstehen, der gefunden wird, wenn man $x_1^{\nu_1} x_2^{\nu_2} \dots x_n^{\nu_n}$ allen Permutationen der symmetrischen Gruppe unterwirft und die Summe aller dieser Ausdrücke bildet, dabei aber mehrfach auftretende fortläßt. Anders ausgedrückt:

$$\sum x_1^{\nu_1} x_2^{\nu_2} \dots x_n^{\nu_n}$$

ist die Summe des Systems der mit $x_1^{\nu_1} x_2^{\nu_2} \dots x_n^{\nu_n}$ konjugierten Funktionen.

Bei $\sum x_1^{\nu_1} x_2^{\nu_2} \dots x_n^{\nu_n}$ kann man das Glied, dessen Exponenten den Ungleichungen $\nu_1 \geqq \nu_2 \geqq \nu_3 \dots \geqq \nu_n$ genügen, zum Anfangsglied wählen. Ist dies geschehen, so bezeichnet man $\sum x_1^{\nu_1} x_2^{\nu_2} \dots x_n^{\nu_n}$ nur durch Angabe der Exponenten $(\nu_1, \nu_2, \dots, \nu_n)$ (G. Cramer, *Introduction à l'analyse des lignes courbes,* Genf 1750, p. 666, Vandermonde, *Résolution des équations* (1771), deutsche Ausg., Berlin 1888, S. 9). Man nennt $(\nu_1, \nu_2, \dots, \nu_n)$ eine *typische, einfache* oder *eintypige symmetrische Funktion.* Von zwei typischen symmetrischen Funktionen $(\nu_1, \nu_2, \dots, \nu_n)$ und $(\nu_1', \nu_2', \dots \nu_n')$ heißt die *erste von höherer Ordnung als die zweite*, wenn in der Zahlenreihe $\nu_1 - \nu_1', \nu_2 - \nu_2', \dots, \nu_n - \nu_n'$ die erste nicht verschwindende Differenz positiv ist, also entweder $\nu_1 > \nu_1'$ oder $\nu_1 = \nu_1', \nu_2 > \nu_2'$ oder $\nu_1 = \nu_1', \nu_2 = \nu_2', \nu_3 > \nu_3'$, usw. (Gauß, *Zweiter Beweis des Fundamentalsatzes*

der Algebra (1815), *Ges. Werke* **3**, 36, *Ostwalds Klassiker der exakten Wiss.* Nr. 14, herausg. von Netto, S. 40.)

Die typischen symmetrischen Funktionen niedrigster Ordnung sind:

$$S_1 = (1, 0, 0, \ldots, 0) = \sum x_1 = x_1 + x_2 + \cdots + x_n,$$
$$S_2 = (1, 1, 0, 0, \ldots, 0) = \sum x_1 x_2 = x_1 x_2 + x_1 x_3 + \cdots + x_1 x_n + x_2 x_3 + \cdots + x_{n-1} x_n,$$
$$S_3 = (1, 1, 1, 0, \ldots, 0) = \sum x_1 x_2 x_3 = x_1 x_2 x_3 + x_1 x_2 x_4 + \cdots + x_{n-2} x_{n-1} x_n,$$
$$\vdots$$
$$S_n = (1, 1, 1, \ldots, 1) = x_1 x_2 x_3 \ldots x_n.$$

Die n Funktionen $S_1, S_2, \ldots, S_n$ heißen die *elementaren symmetrischen* oder die *symmetrischen Grundfunktionen.*

Jede symmetrische ganze Funktion $G(x_1, x_2, \ldots, x_n)$ läßt sich als eine Summe typischer symmetrischer Funktionen der Form $(\nu_1, \nu_2, \ldots, \nu_n)$ mit von den Größen $x_1, x_2, \ldots, x_n$ unabhängigen Zahlenkoeffizienten $M_{\nu_1 \nu_2 \cdots \nu_n}$ darstellen,

$$G = \sum M_{\nu_1 \nu_2 \cdots \nu_n} (\nu_1, \nu_2, \ldots, \nu_n).$$

Es ist (Waring, *Meditationes algebraicae* (1782), 3. ed., p. 13)

$$(\nu_1, \nu_2, \ldots, \nu_n) = S_1^{\nu_1 - \nu_2} S_2^{\nu_2 - \nu_3} \ldots S_n^{\nu_n} + G_1;$$

hierbei bedeutet G_1 eine symmetrische Funktion, die sich nur aus typischen symmetrischen Funktionen *niedrigerer Ordnung* als $(\nu_1, \nu_2, \ldots, \nu_n)$ zusammensetzt. Hieraus ergibt sich der Hauptsatz (Cramer, Vandermonde, Waring, a. a. O., Gauß, *Ges. Werke* **3**, 36, *Ostwalds Klassiker der exakten Wiss.* Nr. 14, S. 40, Cauchy, *Exercices de math.* **4** (1829), *Œuvres* (2) **9**, 132, Kronecker, *Ges. Werke* **1**, 323, **2**, 290):

Jede ganze symmetrische Funktion der Größen $x_1, x_2, \ldots, x_n$ mit ganzzahligen Koeffizienten ist auf eine und auch nur auf eine Weise als ganze ganzzahlige Funktion der symmetrischen Grundfunktionen $S_1, S_2, \ldots, S_n$ darstellbar.

Im besonderen drücken sich die ganzen *Potenzsummen*

$$s_\nu = (\nu, 0, 0, \ldots, 0) = x_1^\nu + x_2^\nu + \cdots + x_n^\nu$$

in der Form

$$s_\nu = \nu \sum (-1)^{\lambda_2 + \lambda_4 + \lambda_6 + \cdots} \frac{(\lambda_1 + \lambda_2 + \cdots + \lambda_n - 1)!}{\lambda_1 ! \, \lambda_2 ! \ldots \lambda_n !} S_1^{\lambda_1} S_2^{\lambda_2} \ldots S_n^{\lambda_n}$$

aus; hierbei ist das Summenzeichen rechter Hand über alle po-

sitiven ganzen Zahlen einschließlich 0 *zu erstrecken, die der Gleichung* $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \cdots + n\lambda_n = \nu$ *genügen* (Waringsche *Formeln*, *Miscellanea analytica* (1762), vgl. Saalschütz, *Bibliotheca math.* (3) **9**, 65 (1908)). Als Umkehrung ergibt sich (Waring, *Miscellanea analytica*):

$$S_\nu = \sum \frac{(-1)^{\nu+\lambda_1+\lambda_2+\cdots+\lambda_\nu}}{1^{\lambda_1}\cdot 2^{\lambda_2}\cdot 3^{\lambda_3}\ldots \nu^{\lambda_\nu}} \frac{1}{\lambda_1!\,\lambda_2!\ldots\lambda_\nu!}\cdot s_1^{\lambda_1} s_2^{\lambda_2}\ldots s_\nu^{\lambda_\nu};$$

hierbei ist $\lambda_1 + 2\lambda_2 + \cdots + \nu\lambda_\nu = \nu$.

Die Darstellung der typischen symmetrischen Funktionen durch die ganzen Potenzsummen wird durch die ebenfalls sogenannten *Waringschen Formeln* gegeben (Waring, *Miscellanea analytica* (1762)). Sie lauten

$$(\nu_1, \nu_2, 0, 0, \ldots, 0) = s_{\nu_1}\cdot s_{\nu_2} - s_{\nu_1+\nu_2} \quad (\nu_1 \neq \nu_2),$$
$$(\nu_1, \nu_1, 0, 0, \ldots, 0) = \tfrac{1}{2}s_{\nu_1}^2 - \tfrac{1}{2}s_{2\nu_1}, \quad \text{usw.}$$

Diese Formeln hat Faà di Bruno, *Einleitung in die Theorie der binären Formen,* deutsch von Walter, Leipzig 1881, S. 8 in die Form folgender symbolischer Determinante gebracht:

$$(\nu_1, \nu_2, \ldots, \nu_k, 0, 0, 0\ldots, 0) = \begin{vmatrix} s_{\nu_1} & s^{\nu_1} & s^{\nu_1} & \ldots & s^{\nu_1} \\ s^{\nu_2} & s_{\nu_2} & s^{\nu_2} & \ldots & s^{\nu_2} \\ \vdots & \vdots & \vdots & & \vdots \\ s^{\nu_k} & s^{\nu_k} & s^{\nu_k} & \ldots & s_{\nu_k} \end{vmatrix};$$

nach der Entwicklung sind die Exponenten der s durch Indices zu ersetzen. Sind unter den Größen $\nu_1, \nu_2, \ldots, \nu_k$ gleiche vorhanden, so ist für je l gleiche die rechte Seite durch $l!$ zu dividieren.

Über symmetrische Funktionen vergleiche auch das Kapitel über Algebra § 5.

Eine Funktion der n Variablen $x_1, x_2, \ldots, x_n$ heißt *alternierend,* wenn sie bei allen Permutationen der n Zahlen 1, 2, $\ldots, n$ nur ihr Vorzeichen ändert.

Jede alternierende Funktion ist von der Form $G\Delta$, *wobei* G *eine symmetrische Funktion und* Δ *das Differenzenprodukt der* n *Variablen* $x_1, x_2, \ldots, x_n$ *bedeutet* (vgl. S. 68).

Jede zweiwertige Funktion ist von der Form $G_1 + G_2 A$, *wobei* G_1 *und* G_2 *symmetrische Funktionen und* A *eine alternierende Funktion bedeutet. Umgekehrt ist jede Funktion der angegebenen Form zweiwertig.*

Ist $\varphi(x_1, x_2, \ldots, x_n)$ *eine* ϱ*-wertige Funktion, so sind* φ *und die mit* φ *konjugierten Funktionen Wurzeln einer Gleichung* ϱ^{ten} *Grades:*

$$z^\varrho + G_1 z^{\varrho-1} + G_2 z^{\varrho-2} + \cdots + G_\varrho = 0,$$

wobei $G_1, G_2, \ldots, G_\varrho$ *symmetrische Funktionen von* $x_1, x_2, \ldots, x_n$ *bedeuten.*

Ist $\mathfrak{G}$ *die Gruppe der rationalen Funktion* $\varphi(x_1, x_2, \ldots, x_n)$ *der* n *Variablen* $x_1, x_2, \ldots, x_n$ *und bleibt die ebenfalls rationale Funktion* $\psi(x_1, x_2, \ldots, x_n)$ *bei allen Permutationen von* $\mathfrak{G}$ *ungeändert, so ist* ψ *eine rationale Funktion von* φ *mit Koeffizienten, die symmetrische Funktionen von* $x_1, x_2, \ldots, x_n$ *sind* (Lagrange, *Œuvres* **3**, 374 (1770)). *Ist* $\mathfrak{H}_h$ *die zu* ψ *gehörige Gruppe*[1]) *und* $\sigma = \frac{h}{g}$ *der Index der Untergruppe* $\mathfrak{G}_g$ *von* $\mathfrak{H}_h$, *so genügt* φ *einer Gleichung* σ^{ten} *Grades*

$$z^\sigma + G_1 z^{\sigma-1} + G_2 z^{\sigma-2} + \cdots + G_\sigma = 0,$$

wobei $G_1, G_2, \ldots, G_\sigma$ *rationale Funktionen von* ψ *und den symmetrischen Funktionen von* $x_1, x_2, \ldots, x_n$ *bedeuten. Die Wurzeln der Gleichung* σ^{ten} *Grades sind die mit* φ *„in bezug auf die Gruppe* $\mathfrak{H}$ *konjugierten Funktionen", d. h. die verschiedenen aus* $\varphi(x_1, x_2, \ldots, x_n)$ *hervorgehenden Größen, wenn man* φ *den Permutationen der Gruppe* $\mathfrak{H}$ *unterwirft.*

Sieht man $x_1, x_2, \ldots, x_n$ als die Wurzeln einer „allgemeinen" Gleichung n^{ten} Grades an, d. h. einer solchen, deren Koeffizienten willkürliche Größen sind und deren Galoissche Gruppe demnach die symmetrische Permutationsgruppe n^{ten} Grades ist, so erhält man die obigen Sätze als Spezialfälle derjenigen Sätze, die in der Galoisschen Theorie (vgl. *Algebra*) für irgendwelche Gleichungen n^{ten} Grades mit beliebigen speziellen Koeffizienten hergeleitet werden.

Über die zu einer Permutationsgruppe zugehörigen Funktionen sei noch verwiesen auf den Artikel *„Rationale Funktionen der Wurzeln; symmetrische und Affektfunktionen"* von Vahlen in der *Encyklopädie der math. Wiss.* **1**, 449.

---

1) Die Gruppe $\mathfrak{H}$ enthält $\mathfrak{G}$ als Untergruppe oder ist mit $\mathfrak{G}$ identisch. Um die σ verschiedenen mit φ in bezug auf die Gruppe $\mathfrak{H}$ konjugierten Funktionen zu finden, genügt es, die Funktion $\varphi(x_1, x_2, \ldots, x_n)$ je einer Substitution aus den σ Nebengruppen zu unterwerfen, die man erhält, wenn man die Gruppe $\mathfrak{H}$ nach dem Modul $\mathfrak{G}$ zerlegt.

§ 9. Lineare homogene Substitutionsgruppen. Reduzibilität. Endliche und unendliche Gruppen. Invarianten endlicher Gruppen.

Ein System $\mathfrak{G}$ von Matrices gleichen Grades n von nicht verschwindenden Determinanten bildet eine Gruppe, wenn es von der Vollständigkeit ist, daß das Produkt irgend zweier sowie die reziproke zu jeder in $\mathfrak{G}$ enthaltenen Matrix der Gesamtheit $\mathfrak{G}$ angehört. Da zu jeder Matrix eine lineare homogene Substitution und umgekehrt (vgl. S. 82) gehört, so spricht man von einer *Gruppe linearer homogener Substitutionen.* (Eine weitergehende Definition, die nicht das Nichtverschwinden der Determinanten der Matrices fordert, bei Frobenius u. J. Schur, *Sitzungsb. der Berl. Akad.* (1906), 209.) Die Zahl n heißt *der Grad der Substitutionsgruppe.*

Umfaßt $\mathfrak{G}$ die Gesamtheit *aller* linearen homogenen Substitutionen von nicht verschwindenden Determinanten, so heißt $\mathfrak{G}$ die *allgemeine lineare homogene Gruppe*, von der jede lineare homogene Substitutionsgruppe Untergruppe ist.

Die Gruppen linearer homogener Substitutionen lassen sich in *reduzible* und *irreduzible* einteilen. Eine Gruppe $\mathfrak{G}$ linearer homogener Substitutionen n^{ten} Grades heißt *reduzibel*, wenn irgendeine Matrix P von nicht verschwindender Determinante existiert, daß die Matrix jeder Substitution der mit $\mathfrak{G}$ ähnlichen Gruppe $\mathfrak{A} = P\mathfrak{G}P^{-1}$ die Gestalt

$$\begin{matrix} R & 0 \\ S & T \end{matrix}$$

hat, wo die den verschiedenen Substitutionen von $\mathfrak{A}$ zugehörigen Matrices R sämtlich von gleichem, aber von niedrigerem als n^{tem} Grade sind. In dem Fall schreibt man auch: die Gruppe $\mathfrak{A}$ hat die Form

$$\begin{matrix} \mathfrak{A}_{11} & 0 \\ \mathfrak{A}_{21} & \mathfrak{A}_{22}, \end{matrix}$$

wobei $\mathfrak{A}_{11}$ die Gesamtheit aller Matrices R, $\mathfrak{A}_{21}$ aller Matrices S und $\mathfrak{A}_{22}$ aller Matrices T repräsentiert. $\mathfrak{A}_{11}$ und $\mathfrak{A}_{22}$ definieren mit $\mathfrak{G}$ und $\mathfrak{A}$ homomorphe Gruppen. Jede nicht reduzible Gruppe heißt *irreduzibel.*

Jede Gruppe $\mathfrak{G}$ linearer homogener Substitutionen läßt sich mittelst einer Matrix P von nicht verschwindender Determinante in eine ähnliche Gruppe $\mathfrak{A} = P\mathfrak{G}P^{-1}$ transformieren, daß die Matrix jeder Substitution von $\mathfrak{A}$ die Form hat:

$$\begin{matrix} \mathfrak{a}_{11} & 0 & 0 & \dots & 0 \\ \mathfrak{a}_{21} & \mathfrak{a}_{22} & 0 & \dots & 0 \\ \mathfrak{a}_{31} & \mathfrak{a}_{32} & \mathfrak{a}_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ \mathfrak{a}_{i1} & \mathfrak{a}_{i2} & \mathfrak{a}_{i3} & \dots & \mathfrak{a}_{ii} \end{matrix}$$

und sämtliche in der Diagonale stehenden Matrices $\mathfrak{a}_{11}, \mathfrak{a}_{22}, \dots,$ $\mathfrak{a}_{ii}$ *irreduzible Gruppen* definieren. Die Gruppen $\mathfrak{a}_{11}, \mathfrak{a}_{22}, \dots, \mathfrak{a}_{ii}$ heißen die *irreduziblen Bestandteile, die sich bei der Darstellung von $\mathfrak{G}$ in der Form $\mathfrak{A}$ ergeben.*

Wie auch immer eine Gruppe $\mathfrak{G}$ linearer homogener Substitutionen unter Hervorhebung ihrer irreduziblen Bestandteile in eine ähnliche Gruppe transformiert wird, so lassen sich die irreduziblen Bestandteile, die sich bei irgendeiner Darstellung ergeben, den irreduziblen Bestandteilen, die sich bei irgendeiner anderen Darstellung ergeben, eineindeutig so zuordnen, daß zwei zugeordnete irreduzible Teilgruppen gleichviele Variablen haben und ähnliche Gruppen sind. (A. Loewy, *Trans. Am. M. S.* **4**, 44 (1903)). Dieser Satz läßt sich auf folgende Weise verallgemeinern (Frobenius und J. Schur, *Sitzungsber. d. Berl. Akad.* (1906), 215): *Zwei holoedrisch isomorphe Gruppen linearer homogener Substitutionen besitzen dann und nur dann die nämlichen irreduziblen Bestandteile, wenn die Spuren*[1]) *je zweier einander entsprechender Substitutionen der beiden isomorphen Gruppen übereinstimmen.*

Eine Gruppe $\mathfrak{G}$ linearer homogener Substitutionen heißt *vollständig reduzibel*, wenn man wenigstens eine Matrix P von nicht verschwindender Determinante finden kann, daß die zu $\mathfrak{G}$ ähnliche Gruppe $\mathfrak{A} = P\mathfrak{G}P^{-1}$ die besondere Form $\{\mathfrak{a}_{11}, \mathfrak{a}_{22}, \dots, \mathfrak{a}_{ii}\}$:

$$\begin{matrix} \mathfrak{a}_{11} & 0 & 0 & \dots & 0 \\ 0 & \mathfrak{a}_{22} & 0 & \dots & 0 \\ 0 & 0 & \mathfrak{a}_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & \mathfrak{a}_{ii} \end{matrix}$$

1) Unter der Spur einer linearen homogenen Substitution versteht man die Summe der Wurzeln der charakteristischen Funktion der betreffenden Substitution.

hat, also abgesehen von der Diagonale, die lauter irreduzible Gruppen enthält, nur Nullmatrices stehen. *Auch die irreduziblen Gruppen* $(i = 1)$ *werden zu den vollständig reduziblen Gruppen gerechnet.*

Nicht jede Gruppe linearer homogener Substitutionen ist vollständig reduzibel. Jede Gruppe $\mathfrak{G}$ linearer homogener Substitutionen läßt sich durch eine Substitution A von nicht verschwindender Determinante in eine ähnliche Gruppe $\mathfrak{G}^* = A\mathfrak{G}A^{-1}$ überführen, bei der die Matrix jeder Substitution die Form:

$$\begin{matrix} \mathfrak{G}^*_{11} & 0 & 0 & \ldots & 0 \\ \mathfrak{G}^*_{21} & \mathfrak{G}^*_{22} & 0 & \ldots & 0 \\ \mathfrak{G}^*_{31} & \mathfrak{G}^*_{32} & \mathfrak{G}^*_{33} & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ \mathfrak{G}^*_{\mu 1} & \mathfrak{G}^*_{\mu 2} & \mathfrak{G}^*_{\mu 3} & \ldots & \mathfrak{G}^*_{\mu\mu} \end{matrix}$$

hat und $\mathfrak{G}^*_{11}, \mathfrak{G}^*_{22}, \ldots, \mathfrak{G}^*_{\mu\mu}$ *aufeinanderfolgende größte vollständig reduzible Gruppen* bedeuten. *Betrachtet man ähnliche Gruppen linearer homogener Substitutionen als nicht verschieden, so sind die Gruppen* $\mathfrak{G}^*_{11}, \mathfrak{G}^*_{22}, \ldots, \mathfrak{G}^*_{\mu\mu}$ *ihrer Reihenfolge nach als erste, zweite usw. bis* μ^{te} *vollständig reduzible, zu* $\mathfrak{G}$ *gehörige Gruppen eindeutig bestimmt und von der Wahl der überführenden Matrix* A *unabhängig. Zu jeder Gruppe linearer homogener Substitutionen gehört daher eine homomorphe vollständig reduzible Gruppe* $\{\mathfrak{G}^*_{11}, \mathfrak{G}^*_{22}, \ldots, \mathfrak{G}^*_{\mu\mu}\}$ *desselben Grades. Sieht man ähnliche Gruppen als nicht verschieden an, so ist diese ebenso wie ihre irreduziblen Bestandteile*[1] *eindeutig bestimmt.* (A. Loewy, *Trans. Am. M. S.* **6**, 504 (1905), Stickelberger, ebenda **7**, 509 (1906), J. Schur, erscheint ebenda **10** (1909), A. Loewy, *Math. Ann.* **64**, 267 (1907).) Die Gruppe $\mathfrak{G}$ ist dann und nur dann vollständig reduzibel, wenn $\mu = 1$ ist.

Eine Gruppe linearer homogener Substitutionen in n Variablen ist dann und nur dann irreduzibel, wenn aus ihr ein System von n^2 *Substitutionen* $A_j (j = 1, 2, \ldots, n^2)$ *mit Koeffizienten* $a_{ik}^{(j)}$ $(i, k = 1, 2, \ldots, n;\ j = 1, 2, \ldots, n^2)$ *ausgewählt werden kann, daß die Determinante:*

---

1) Die irreduziblen Bestandteile der Gruppe $\mathfrak{G}$ sind die Gesamtheit der irreduziblen Bestandteile der vollständig reduziblen Gruppen $\mathfrak{G}^*_{11}, \mathfrak{G}^*_{22}, \ldots, \mathfrak{G}^*_{\mu\mu}$.

$$\begin{vmatrix} a_{11}^{(1)} & a_{12}^{(1)} & \dots & a_{nn}^{(1)} \\ a_{11}^{(2)} & a_{12}^{(2)} & \dots & a_{nn}^{(2)} \\ \vdots & & & \\ a_{11}^{(n^2)} & a_{12}^{(n^2)} & \dots & a_{nn}^{(n^2)} \end{vmatrix} \neq 0$$

ist. Anders ausgedrückt: Eine Gruppe n^{ten} Grades ist dann und nur dann irreduzibel, wenn unter ihren Matrices n^2 linear unabhängige (vgl. S. 86) *existieren.* (W. Burnside, *Proc. Lond. M. S.* (2) **3**, 430 (1905), Frobenius und J. Schur, *Sitzungsb. d. Berl. Akad.* (1906), 209, Taber, *Math. Ann.* **64**, 357 (1907).)

Die *irreduziblen,* auch *transitiv* genannten Gruppen linearer homogener Substitutionen lassen sich in *primitive* und *imprimitive* einteilen. Eine irreduzible Gruppe linearer homogener Substitutionen heißt *imprimitiv*, wenn sie in eine derartige ähnliche Gruppe transformierbar ist, daß die Variablen in m Systeme von je $\frac{n}{m}$ Variablen zerfallen und alle Variablen eines Systems entweder nur in lineare homogene Funktionen der Variablen des gleichen oder eines anderen Systems übergehen. (Blichfeldt, *Trans. Am. M. S.* **4**, 388 (1903), **6**, 230 (1905)).

Zu den reduziblen Gruppen gehören auch die kommutativen Gruppen linearer homogener Substitutionen; für sie gilt folgendes Theorem: *Jede kommutative Gruppe linearer homogener Substitutionen, die durch q Elemente erzeugt wird, ist reduzibel, und jeder ihrer irreduziblen Bestandteile ist eine Gruppe in einer einzigen Variablen.* Anders ausgedrückt: *Die Matrices aller Substitutionen einer solchen Gruppe lassen sich durch eine und dieselbe Matrix in dreieckige Form transformieren, so daß rechter Hand von der Diagonale ausschließlich Nullen auftreten.* (Frobenius, *Sitzungsb. d. Berl. Akad.* (1896), 601, J. Schur, ebenda (1902), 120, H. Weber, *Algebra* **2**, 176, Dickson, *Quart. J.* **40**, 167 (1909).) *Die Anzahl der linear unabhängigen Matrices einer kommutativen Gruppe linearer homogener Substitutionen n^{ten} Grades ist höchstens*

$$\left[\frac{n^2}{4}\right] + 1,$$

wobei $\left[\frac{n^2}{4}\right]$ die größte in $\frac{n^2}{4}$ enthaltene ganze Zahl ist. (J. Schur, *Journ. f. Math.* **130**, 66 (1905).)

Die Gruppen linearer homogener Substitutionen werden in *endliche* und *unendliche* unterschieden. Eine Gruppe $\mathfrak{G}$ linearer

homogener Substitutionen heißt von der *endlichen Ordnung g*, wenn sie nur die endliche Anzahl g linearer homogener Substitutionen umfaßt.

Bei jeder endlichen Gruppe $\mathfrak{G}$ linearer homogener Substitutionen ist jede einzelne Substitution von endlicher Ordnung. Umgekehrt: *Weiß man, daß alle Substitutionen einer Gruppe linearer homogener Substitutionen von niedrigerer als* q^{ter} *Ordnung sind, wobei* q *irgendeine positive Zahl ist, so ist die Gruppe endlich. Eine unendliche Gruppe linearer homogener Substitutionen muß wenigstens eine Substitution unendlich hoher Ordnung enthalten.* (A. Loewy, *Math. Ann.* **53**, 225 (1900), **64**, 264 (1907), W. Burnside, *Proc. Lond. M. S.* (2) **3**, 435 (1905).)

Eine lineare homogene Substitution ist dann und nur dann von endlicher Ordnung, wenn ihre charakteristische Funktion bloß für Einheitswurzeln verschwindet und sämtliche Elementarteilerexponenten gleich 1 *sind. Die Matrix einer jeden linearen homogenen Substitution* n^{ten} *Grades von endlicher Ordnung* s *ist daher mit der zerlegbaren Matrix* $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n\}$ *ähnlich* (vgl. S. 92), *wobei* $\varepsilon_i^s = 1$ $(i = 1, 2, \ldots, n)$ *ist.* (Frobenius, *Journ. f. Math.* **84**, 16 (1878), *Sitzungsb. d. Berl. Akad.* (1896), 607, C. Jordan, *Journ. f. Math.* **84**, 112 (1878), vgl. auch H. Weber, *Algebra* **2**, 186.)

Jede endliche Gruppe linearer homogener Substitutionen führt eine definite Hermitesche Form (d. h. eine Hermitesche Form (vgl. S. 128), die nur verschwindet, wenn sämtliche Variablen gleich Null gesetzt werden) *in sich über.* (A. Loewy. *C. R.* **123**, 168 (1896), E. H. Moore, *Math. Ann.* **50**, 213 (1898).) Die verwandten Untersuchungen von L. Fuchs, *Sitzungsb. d. Berl. Akad.* (1896), 753 sind fehlerhaft; vgl. die Bemerkungen von Schlesinger zu diesem Aufsatz in *Fuchs' Ges. Werken* **3** (erscheint nächstens).

Jede endliche Gruppe linearer homogener Substitutionen ist vollständig reduzibel. (H. Maschke, *Math. Ann.* **52**, 363 (1899), W. Burnside, *Acta math.* **28**, 377 (1904), J. Schur, *Sitzungsb. d. Berl. Akad.* (1905), 414, A. Loewy, *Trans. Am. M. S.* **6**, 509 (1905).)

Bisher ist keine endliche Gruppe linearer homogener Substitutionen g^{ter} Ordnung bekannt, die nicht einer solchen ähnlich ist, deren Koeffizienten ausnahmslos dem Zahlkörper der g^{ten} Einheitswurzeln angehören. (Über die erzielten Resultate vgl. Maschke, *Math. Ann.* **50**, 492 (1898), W. Burnside,

Proc. Lond. M. S. (2) **3**, 239 (1905), J. Schur, *Sitzungsb. d. Berl. Akad.* (1906), 164.)

Jede endliche Gruppe linearer homogener Substitutionen von Primzahlpotenzordnung ist einer Gruppe mit Substitutionen der Form (sog. Monomialgruppe) $x_i' = a_i x_{\lambda_i}$ $(i = 1, 2, \ldots, n)$ *ähnlich, wobei* $a_1, a_2, \ldots, a_n$ *Konstante sind und* $\lambda_1, \lambda_2, \ldots, \lambda_n$ *bis auf die Reihenfolge die Zahlen* 1, 2, ..., n *bedeuten.* (Blichfeldt, *Trans. Am. M. S.* **5**, 313 (1904).)

Satz von C. Jordan (*Journ. f. Math.* **84**, 91 (1878)):

Jede endliche Gruppe $\mathfrak{G}$ *linearer homogener Substitutionen in* n *Variablen besitzt eine invariante kommutative Untergruppe* $\mathfrak{J}$ *von der Beschaffenheit, daß der Quotient* $\lambda = \frac{g}{i}$ *der Ordnungen von* $\mathfrak{G}$ *und* $\mathfrak{J}$ *kleiner als eine nur durch* n *allein bestimmte Zahl ist.* Neuer Beweis mit Bestimmung einer oberen Grenze für λ bei Blichfeldt, *Trans. Am. M. S.* **4**, 387 (1903), **5**, 310 (1904), **6**, 230 (1905). Die Ordnung $g = \lambda i$ kann beliebig große Werte annehmen (vgl. J. Schur, *Sitzungsb. d. Berl. Akad.* (1905), 77).

Eine ganze homogene Funktion $\Phi(x_1 x_2 \ldots x_n)$ der n Variablen $x_1, x_2, \ldots, x_n$ (Form) heißt eine *Invariante einer Gruppe* $\mathfrak{G}$ *linearer homogener Substitutionen*, wenn sie bis auf einen von den Variablen $x_1, x_2, \ldots, x_n$ unabhängigen Faktor ungeändert bleibt, falls man die x_i allen Substitutionen der Gruppe unterwirft. Man unterscheidet zwischen *relativen* und *absoluten Invarianten einer Gruppe* $\mathfrak{G}$. *Die Faktoren, mit denen sich eine relative Invariante einer Gruppe* $\mathfrak{G}$ *linearer homogener Substitutionen von der endlichen Ordnung* g *multiplizieren kann, sind ausnahmslos* g^{te} *Einheitswurzeln. Sind alle Faktoren, mit denen sich eine relative Invariante* $\Phi(x_1, x_2, \ldots, x_n)$ *einer* $\mathfrak{G}_g$ *multipliziert,* e^{te} *Einheitswurzeln und ist wenigstens ein Faktor auch keine niedrigere als* e^{te} *Einheitswurzel, so heißt* Φ *eine Invariante der Gruppe* $\mathfrak{G}$ *vom Index* e*; die Gruppe* $\mathfrak{G}$ *enthält alsdann eine invariante Untergruppe* $\mathfrak{J}$*, und der Index von* $\mathfrak{J}$ *in bezug auf* $\mathfrak{G}$ *ist gleich* e.

Ein System von Formen heißt endlich, wenn sich jede Form des Systems als ganze rationale Funktion einer endlichen Anzahl von Formen, die ebenfalls dem System angehören, darstellen läßt. Diese endliche Anzahl von Formen, durch die sich jede Form des Systems in ganzer rationaler Weise ausdrücken läßt, heißt ein *volles Formensystem.*

Das System aller Invarianten jeder endlichen Gruppe linearer homogener Substitutionen ist endlich. Das System aller absoluten

Invarianten jeder endlichen Gruppe linearer homogener Substitutionen ist endlich. (Hilberts Satz von der Endlichkeit des Invariantensystems einer endlichen Gruppe, Hilbert, *Math. Ann.* **36**, 473 (1890), H. Weber, *Algebra* **2**, 218.)

Unter den Invarianten jeder endlichen Gruppe linearer homogener Substitutionen, die relative Invarianten besitzt, kann man m Invarianten $\Psi_1, \Psi_2, \ldots, \Psi_m$ derartig auswählen, daß jede Invariante der Gruppe von der Form: $\Phi_1 \Psi_1 + \Phi_2 \Psi_2 + \cdots \Phi_m \Psi_m$ wird, wobei $\Phi_1, \Phi_2, \ldots, \Phi_m$ absolute Invarianten sind.

Ist $\mathfrak{G}$ die symmetrische Gruppe $\mathfrak{S}_{n!}$ von n Symbolen, so bilden die symmetrischen Grundfunktionen $S_1, S_2, \ldots, S_n$ ein volles System absoluter Invarianten, das Differenzenprodukt Δ ist eine relative Invariante vom Index 2 und bildet mit S_1, $S_2, \ldots, S_n$ ein volles System aller Invarianten von $\mathfrak{S}_{n!}$ (Hieraus ergeben sich auch die Sätze auf S. 219 u. 220.)

Als Aufgabe der Algebra kann angesehen werden: Man soll die Unbekannten $x_1, x_2, \ldots, x_n$ finden, wenn die Invarianten $S_1, S_2, \ldots, S_n$ gegeben sind. Es handelt sich um die Bestimmung der Wurzeln der Gleichung:

$$z^n - S_1 z^{n-1} + S_2 z^{n-2} - S_3 z^{n-3} \cdots (-1)^n S_n = 0 .$$

Klein (*Math. Ann.* **15**, 253 (1879), *The Evanston Colloquium, Lectures on mathematics*, New York 1894, S. 72) hat dieses Problem dahin erweitert: *Für unbekannte $x_1, x_2, \ldots, x_n$ seien die Werte eines vollen Systems absoluter Invarianten einer endlichen linearen homogenen Substitutionsgruppe $\mathfrak{G}$ in Übereinstimmung mit den zwischen ihnen bestehenden Relationen*[1]) *gegeben: man soll $x_1, x_2, \ldots, x_n$ bestimmen. Die Bestimmung der Variablen $x_1, x_2, \ldots, x_n$ hängt von einer Normalgleichung ab, deren Galoissche Gruppe mit $\mathfrak{G}$ holoedrisch isomorph ist.* (Vgl. H. Weber, *Algebra* **2**, 228.)

§ 10. Darstellung einer endlichen abstrakten Gruppe als Permutationsgruppe und als Gruppe linearer homogener Substitutionen.

Jede Permutationsgruppe, die mit einer gegebenen endlichen abstrakten Gruppe holoedrisch oder meroedrisch isomorph ist, bezeichnet man als eine *Darstellung der abstrakten Gruppe*

1) Zwischen $n+1$ Invarianten einer $\mathfrak{G}$ n^{ten} Grades muß stets eine rationale Gleichung bestehen, wie sich durch Elimination der n Variablen x_i $(i = 1, 2, \ldots, n)$ aus den $n+1$ homogenen ganzen Funktionen ergibt.

als Permutationsgruppe. Sind $G_1, G_2, \ldots, G_g$ die Elemente einer endlichen abstrakten Gruppe $\mathfrak{G}$ und ordnet man dem Element G_i entweder die Permutation

$$\begin{pmatrix} G_1 & G_2 & \ldots & G_g \\ G_1 G_i & G_2 G_i & \ldots & G_g G_i \end{pmatrix}$$

oder

$$\begin{pmatrix} G_1 & G_2 & \ldots & G_g \\ G_i^{-1} G_1 & G_i^{-1} G_2 & \ldots & G_i^{-1} G_g \end{pmatrix}$$

zu, so hat man zwei mit $\mathfrak{G}$ holoedrisch isomorphe reguläre Permutationsgruppen. Jede Permutation der einen Gruppe ist mit jeder der anderen vertauschbar. (Cayley, *Am. J. math.* **1**, 52 (1878), *Coll. math. papers* **10**, 403, Frobenius u. Stickelberger, *Journ. f. Math.* **86**, 230 (1879), Dyck, *Math. Ann.* **22**, 84 (1883).)

Hat die Gruppe $\mathfrak{G}$ der Ordnung g die Gruppe $\mathfrak{H}$ der Ordnung h zur Untergruppe und ist $\mathfrak{J}$ die größte in $\mathfrak{H}$ enthaltene invariante Untergruppe von $\mathfrak{G}$, so ist $\mathfrak{G}/\mathfrak{J}$ als holoedrisch isomorphe transitive Permutationsgruppe $\mathfrak{h}$ in $\frac{g}{h}$ Symbolen darstellbar. Ist die größte in $\mathfrak{H}$ enthaltene invariante Untergruppe von $\mathfrak{G}$ die Einheit, so ist $\mathfrak{h}$ eine holoedrisch isomorphe Darstellung von $\mathfrak{G}$ selbst. In diesem Fall ist $\mathfrak{h}$ eine primitive Permutationsgruppe, wenn es keine Gruppe $\mathfrak{A}$ gibt, die in $\mathfrak{G}$ enthalten ist und $\mathfrak{H}$ enthält; existiert eine derartige Gruppe $\mathfrak{A}$, so ist $\mathfrak{h}$ imprimitiv. (Dyck, *Math. Ann.* **22**, 94 (1883), Frobenius, *Sitzungsb. d. Berl. Akad.* (1895), 179.)

Jede einfache Gruppe ist als holoedrisch isomorphe primitive Permutationsgruppe darstellbar. Eine solche Darstellung erhält man nach dem vorigen Satz, indem man $\mathfrak{H}$ als Maximaluntergruppe von $\mathfrak{G}$ wählt.

Über die Darstellbarkeit einer endlichen abstrakten Gruppe als Permutationsgruppe vgl.: W. Burnside, *Proc. Lond. M. S.* **34**, 159 (1902), G. A. Miller, *Giornale di mat.* **38**, 63 (1900).

Sind $G_1, G_2, \ldots, G_g$ die g Elemente einer endlichen abstrakten Gruppe $\mathfrak{G}$, so heißen g Matrices (lineare homogene Substitutionen) gleichen Grades $(G_1), (G_2), \ldots, (G_g)$, die bei ihrer Komposition den g^2 Relationen: $(R)(S) = (RS)$ genügen, wenn R und S alle Elemente aus $\mathfrak{G}$ durchlaufen, eine *Dar-*

stellung der Gruppe 𝔊 *durch lineare homogene Substitutionen;* hierbei brauchen die Matrices $(G_1), (G_2), \ldots, (G_g)$ nicht sämtlich untereinander verschieden zu sein. Verschwinden die Determinanten der Matrices $(G_1), (G_2), \ldots, (G_g)$ nicht, so definieren $(G_1), (G_2), \ldots, (G_g)$ eine *mit der abstrakten Gruppe* 𝔊 *homomorphe Gruppe linearer homogener Substitutionen.*

Die Anzahl verschiedener, d. h. nicht untereinander ähnlicher, mit der Gruppe 𝔊 *homomorpher irreduzibler Gruppen linearer homogener Substitutionen ist endlich und gleich der Zahl k von Klassen konjugierter Elemente von* 𝔊. *Der Grad jeder dieser Substitutionsgruppen ist ein Divisor der Ordnung der Gruppe* 𝔊.

Bildet das System von Matrices n^{ten} Grades $(G_1), (G_2), \ldots, (G_g)$ eine Darstellung der abstrakten Gruppe 𝔊 und bedeuten x_{G_i} $(i = 1, 2, \ldots, g)$ g unabhängige Variable, so heißt die Matrix $\sum\limits_R (R) x_R$ $(R = G_1, G_2, \ldots, G_g)$ die *dieser Darstellung entsprechende Gruppenmatrix oder eine zur Gruppe* 𝔊 *gehörige Matrix.* Die zu einer irreduziblen Gruppe linearer homogener Substitutionen gehörige Gruppenmatrix heißt eine *irreduzible Gruppenmatrix.* Ist X irgendeine Gruppenmatrix und A eine konstante Matrix von nicht verschwindender Determinante, so ist die ähnliche Matrix AXA^{-1} ebenfalls eine Gruppenmatrix. Sieht man ähnliche irreduzible Gruppenmatrices als nicht verschieden an, so gibt es entsprechend den k verschiedenen mit einer abstrakten Gruppe 𝔊 homomorphen irreduziblen Gruppen linearer homogener Substitutionen genau k *irreduzible zur Gruppe* 𝔊 *gehörige irreduzible Gruppenmatrices.*

Jede Gruppenmatrix X des Grades n und des Ranges r läßt sich in eine ähnliche Gruppenmatrix: $\{U_1, U_2, \ldots, U_m, N_{n-r}\}$ (vgl. die Symbolik auf S. 92) *transformieren, so daß $U_1, U_2, \ldots, U_m$ irreduzible Gruppenmatrices bedeuten und N_{n-r} die Nullmatrix des Grades $n - r$ ist. Wenn man ähnliche irreduzible Gruppenmatrices als nicht verschieden ansieht, entspricht auf diese Weise jeder Gruppenmatrix ein bis auf die Reihenfolge eindeutig bestimmtes System irreduzibler Gruppenmatrices $U_1, U_2, \ldots, U_m$; dieses enthält nur Matrices aus den k zur Gruppe* 𝔊 *gehörigen irreduziblen Gruppenmatrices und diese eventuell auch mehrfach.*

Die Koeffizienten irgendeiner Gruppenmatrix

$$X = \sum (R) x_R = \| x_{ik} \| \qquad (i, k = 1, 2, \ldots, n)$$

sind lineare homogene Funktionen der Variablen $x_{G_1}, x_{G_2}, \ldots, x_{G_g}$. Ist $y_{G_1}, y_{G_2}, \ldots, y_{G_g}$ ein zweites System g unabhängiger Variablen, und setzt man

$$z_R = \sum_S x_S y_{S^{-1}R} \quad (R, S = G_1, G_2, \ldots, G_g),$$

so besteht die Gleichung $Z = XY$, falls Y und Z die Matrices bedeuten, die aus X hervorgehen, wenn man die Variablen x_R durch y_R bzw. z_R ersetzt.

Jede Permutationsgruppe läßt sich als eine Gruppe linearer homogener Substitutionen auffassen. Infolgedessen gehören zu den am Anfang dieses Paragraphen besprochenen Darstellungen der abstrakten Gruppe $\mathfrak{G}$ durch zwei reguläre Permutationsgruppen auch zwei Gruppenmatrices, nämlich

$$X_1 = \| x_{G_i^{-1} G_k} \| \quad \text{und} \quad X_2 = \| x_{G_i G_k^{-1}} \|.$$

Die Matrix X_2, deren Zeilen und Kolonnen man erhält, indem man füx G_i und G_k der Reihe nach die Elemente $G_1, G_2, \ldots, G_g$ setzt, heißt die *reguläre Gruppenmatrix.* Die zu X_1 transponierte Matrix $X_1' = \| x_{G_k^{-1} G_i} \|$ heißt die *antistrophe Matrix.* Ist Y_1' die aus X_1' hervorgehende Matrix, wenn man die Variablen $x_{G_1}, x_{G_2}, \ldots, x_{G_g}$ durch $y_{G_1}, y_{G_2}, \ldots, y_{G_g}$ ersetzt, so besteht die Gleichung $Y_1' X_2 = X_2 Y_1'$. *Die Elemente $G_1, G_2, \ldots, G_g$ einer endlichen abstrakten Gruppe $\mathfrak{G}$ lassen sich als die g Einheiten eines Systems höherer komplexer Zahlen auffassen.* Daher findet man auch die reguläre Gruppenmatrix X_2 und die Matrix Y_1' durch Spezialisierung der Matrices $\mathfrak{G}$ und $\mathfrak{H}'$ auf S. 99.

Die Determinante der regulären Gruppenmatrix X_2 ist nicht identisch Null; daher transformiert sich X_2 in $\{U_1, U_2, \ldots, U_m\}$, und es tritt keine Nullmatrix auf. *Hat man die reguläre Gruppenmatrix, so sind unter $U_1, U_2, \ldots, U_m$ sämtliche k irreduziblen Gruppenmatrices, und zwar jede so oft, als ihr Grad angibt, enthalten. Die Bestimmung aller Darstellungen einer endlichen abstrakten Gruppe durch ganze lineare homogene Substitutionen ist daher mit der Aufgabe identisch, die reguläre Gruppenmatrix in irreduzible Bestandteile zu zerfällen.*

Bilden $(G_1), (G_2), \ldots (G_g)$ eine Darstellung der endlichen Gruppe $\mathfrak{G}$ und ist $\chi(R)$ die Spur der Substitution (R), d. h. die Summe der Wurzeln der charakteristischen Funktion der Substitution (R), so heißt das System der g Zahlen $\chi(R)$, das höchstens k untereinander verschiedene enthält, wenn (R) die

Matrices (G_1), (G_2), ..., (G_g) durchläuft, der *Gruppencharakter*, der dieser Darstellung oder ihrer zugehörigen Gruppenmatrix entspricht. Ein einer irreduziblen Gruppenmatrix entsprechender Gruppencharakter heißt ein *einfacher Gruppencharakter*. Unter den Zahlen eines einfachen Gruppencharakters befindet sich auch die der Einheit (E) der Gruppe zugeordnete Zahl $\chi(E)$, die den Grad der irreduziblen Gruppe angibt.

Zwei Darstellungen einer endlichen Gruppe $\mathfrak{G}$ durch lineare homogene Substitutionen von nicht verschwindenden Determinanten sind dann und nur dann ähnlich, wenn sie denselben Gruppencharakter besitzen. (Spezialfall des oben S. 223 angegebenen Satzes über isomorphe unendliche Gruppen linearer homogener Substitutionen von Frobenius u. J. Schur, *Sitzungsb. d. Berl. Akad.* (1906), 215.)

Eingehend untersucht ist die Darstellung der symmetrischen und alternierenden Gruppe durch Gruppen linearer homogener Substitutionen (Frobenius, *Sitzungsb. d. Berl. Akad.* (1900), 516, (1903), 328). *Jede Gruppe linearer homogener Substitutionen, die der symmetrischen Permutationsgruppe in n Symbolen homomorph ist, läßt sich durch eine lineare Transformation der Variablen in eine ähnliche Gruppe mit ganzzahligen rationalen Koeffizienten überführen.* (J. Schur, *Sitzungsb. d. Berl. Akad.* (1908), 664.)

Das Problem, die Darstellungen einer endlichen abstrakten Gruppe durch lineare homogene Substitutionen zu finden, ist zuerst von Frobenius, *Sitzungsb. d. Berl. Akad.* (1896), 985 u. 1343, (1897), 994, (1899), 482, (1903), 328, 401 und Molien, *Sitzungsb. d. naturforsch. Gesellsch. zu Dorpat* (1897), 259 durchgeführt worden. Vgl. besonders die elementare Darstellung von J. Schur, *Sitzungsb. d. Berl. Akad.* (1905), 406, ferner W. Burnside, *Acta math.* **28**, 369 (1904), *Proc. Lond. M. S.* (2) **1**, 117 (1904), H. Weber, *Algebra* **2**, 193. In dem Problem, alle mit einer abstrakten Gruppe $\mathfrak{G}$ homomorphen Gruppen linearer homogener Substitutionen zu bestimmen, ist im besonderen das von F. Klein (*The Evanston Colloquium, Lectures on mathematics*, New York 1894, S. 73) sogenannte *Normalproblem* enthalten, das die Bestimmung aller mit einer Gruppe isomorphen linearen homogenen Substitutionsgruppen niedrigsten Grades verlangt.

§ 11. Kollineationsgruppen. Darstellbarkeit einer endlichen abstrakten Gruppe als Kollineationsgruppe. Die verschiedenen Typen endlicher Kollineationsgruppen in einer, zwei und drei Variablen.

Aus zwei linear gebrochenen Substitutionen:

$$A_1 : \xi_i = \frac{a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in-1}\xi_{n-1}' + a_{in}}{a_{n1}\xi_1' + a_{n2}\xi_2' + \cdots + a_{nn-1}\xi_{n-1}' + a_{nn}} \quad (i=1,2,\ldots,n-1)$$

$$B_1 : \xi_i' = \frac{b_{i1}\xi_1'' + b_{i2}\xi_2'' + \cdots + b_{in-1}\xi_{n-1}'' + b_{in}}{b_{n1}\xi_1'' + b_{n2}\xi_2'' + \cdots + b_{nn-1}\xi_{n-1}'' + b_{nn}} \quad (i=1,2,\ldots,n-1)$$

in $n-1$ Variablen entspringt eindeutig eine dritte, ihr *Produkt* $C_1 = A_1 B_1$:

$$C_1 : \xi_i = \frac{c_{i1}\xi_1'' + c_{i2}\xi_2'' + \cdots + c_{in-1}\xi_{n-1}'' + c_{in}}{c_{n1}\xi_1'' + c_{n2}\xi_2'' + \cdots + c_{nn-1}\xi_{n-1}'' + c_{nn}} \quad (i=1,2,\ldots,n-1),$$

wobei $c_{ik} = \sum_{s=1}^{s=n} a_{is} b_{sk} \quad (i,k=1,2,\ldots,n)$.

Verschwindet die Determinante $|a_{ik}|$ $(i,k=1,2,\ldots,n)$ nicht, so existiert zu A_1 eine reziproke Substitution:

$$A_1^{-1} : \xi_i' = \frac{A_{1i}\xi_1 + A_{2i}\xi_2 + \cdots + A_{n-1\,i}\xi_{n-1} + A_{ni}}{A_{1n}\xi_1 + A_{2n}\xi_2 + \cdots + A_{n-1\,n}\xi_{n-1} + A_{nn}} \quad (i=1,2,\ldots,n-1),$$

wobei die Größen $A_{ik} = \frac{\partial |a_{ik}|}{\partial a_{ik}}$ die Unterdeterminanten von $|a_{ik}|$ $(i,k=1,2,\ldots,n)$ bedeuten. Den Grad n der Matrix $\|a_{ik}\|$ bezeichnet man als den *Grad der Substitution* A_1.

Eine Gesamtheit $\mathfrak{G}_1$ linear gebrochener Substitutionen von gleichem Grad und nicht verschwindenden Determinanten bildet eine Gruppe, wenn sie von der Vollständigkeit ist, daß das Produkt irgend zweier sowie die reziproke zu jeder in $\mathfrak{G}_1$ enthaltenen Substitution ebenfalls der Gesamtheit $\mathfrak{G}_1$ angehört. *Eine Gruppe linear gebrochener Substitutionen heißt eine Kollineationsgruppe* oder *projektive Gruppe.* Umfaßt die Gruppe $\mathfrak{G}_1$ die Gesamtheit *aller* linear gebrochenen Substitutionen von gleichem Grad und nicht verschwindenden Determinanten, so heißt $\mathfrak{G}_1$ die *allgemeine projektive Gruppe* (vgl. S. 175) oder die *allgemeinste Kollineationsgruppe*, von der jede Gruppe linear gebrochener Substitutionen Untergruppe ist. Im besonderen gehört zu den Untergruppen der allgemeinen projektiven Gruppe die *allgemeine lineare unhomogene Substitutionsgruppe* in $n-1$

Variablen, auch die *volle lineare Gruppe* in $n-1$ Variablen genannt; sie besteht aus allen Substitutionen:

$$\xi_i = a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in-1}\xi_{n-1}' + a_{in} \qquad (i = 1, 2, \ldots, n-1)$$

mit nicht verschwindenden Determinanten $|a_{ik}|$ $(i, k = 1, 2, \ldots, n-1)$.

Ordnet man den Substitutionen A:

$$x_i = a_{i1}x_1' + a_{i2}x_2' + \cdots + a_{in}x_n' \qquad (i = 1, 2, \ldots, n)$$

einer Gruppe $\mathfrak{G}$ linearer homogener Substitutionen die linear gebrochenen Substitutionen A_1:

$$\xi_i = \frac{a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in-1}\xi_{n-1}' + a_{in}}{a_{n1}\xi_1' + a_{n2}\xi_2' + \cdots + a_{nn-1}\xi_{n-1}' + a_{nn}} \qquad (i = 1, 2, \ldots, n-1)$$

zu, so erhält man eine mit $\mathfrak{G}$ homomorphe Kollineationsgruppe $\mathfrak{G}_1$, die zu $\mathfrak{G}$ *zugehörige Kollineationsgruppe* $\mathfrak{G}_1$. Ist Γ die Gruppe aller in $\mathfrak{G}$ etwa enthaltenen Ähnlichkeitstransformationen: $x_i = \nu x_i'$ $(i = 1, 2, \ldots, n)$, so sind $\mathfrak{G}/\Gamma$ und $\mathfrak{G}_1$ holoedrisch isomorph.

Nicht jede Kollineationsgruppe $\mathfrak{G}_1$ n^{ten} Grades kann als lineare homogene Gruppe der gleichen Ordnung in n Variablen dargestellt werden; hingegen kann jede Kollineationsgruppe der Ordnung g in $n-1$ Variablen aus einer homomorphen Gruppe linearer homogener Substitutionen der Determinante $+1$ und der Ordnung ng in n Variablen abgeleitet werden. Man erhält sie, indem man jeder linear gebrochenen Substitution mit der Matrix $\|a_{ik}\|$ $(i, k = 1, 2, \ldots, n)$ die n Matrices $\|\alpha_{ik}^{(j)}\|$ $(i, k, j = 1, 2, \ldots, n)$ entsprechen läßt; hierbei ist $\alpha_{ik}^{(j)} = \varepsilon_j \frac{a_{ik}}{\sqrt[n]{|a_{ik}|}}$, wobei ε_j alle n^{ten} Einheitswurzeln durchläuft und $|a_{ik}|$ die Determinante der Matrix $\|a_{ik}\|$ $(i, k = 1, 2, \ldots, n)$ bedeutet.

Zwei Kollineationsgruppen $\mathfrak{G}_1$ und $\mathfrak{G}_2$ heißen *ähnlich, konjugiert, gleichberechtigt* oder *äquivalent*, wenn eine Kollineation P_1 von nicht verschwindender Determinante existiert, so daß $P_1\mathfrak{G}_1P_1^{-1} = \mathfrak{G}_2$ ist.

Die Kollineationsgruppe $\mathfrak{G}_1$ heißt *irreduzibel*, wenn es die zugeordnete homomorphe lineare homogene Substitutionsgruppe ist.

Hat man irgendeine abstrakte endliche Gruppe $\mathfrak{H}$, so kann man sich analog der Aufgabe, alle Darstellungen von $\mathfrak{H}$ durch ganze lineare homogene Substitutionsgruppen zu finden (vgl. S. 229), das Problem stellen, *alle mit $\mathfrak{H}$ homomorphen Kollineationsgruppen* zu bestimmen. Hierzu hat man zuerst eine *Darstellungsgruppe $\mathfrak{D}$ der abstrakten Gruppe $\mathfrak{H}$* aufzusuchen.

Die abstrakte Gruppe $\mathfrak{D}$ heißt eine *Darstellungsgruppe von* $\mathfrak{H}$, wenn sie die Gruppe höchster Ordnung ist, die erstens eine aus invarianten Elementen von $\mathfrak{D}$ bestehende Untergruppe $\mathfrak{M}$ besitzt, so daß die Faktorgruppe $\mathfrak{D}/\mathfrak{M}$ und die Gruppe $\mathfrak{H}$ holoedrisch isomorph sind, zweitens die Kommutatorgruppe von $\mathfrak{D}$ alle Elemente von $\mathfrak{M}$ enthält. Für eine abstrakte Gruppe $\mathfrak{H}$ können auch mehrere nicht isomorphe Darstellungsgruppen existieren. Die endliche kommutative Gruppe $\mathfrak{M}$ ist durch die Gruppe $\mathfrak{H}$ *eindeutig* bestimmt; die Gruppe $\mathfrak{M}$ heißt der *Multiplikator der Gruppe* $\mathfrak{H}$. Hieraus folgt im besonderen, daß alle Darstellungsgruppen einer Gruppe $\mathfrak{H}$ von der gleichen Ordnung sind.

Bestimmt man alle irreduziblen Darstellungen irgend einer abstrakten Darstellungsgruppe $\mathfrak{D}$ *von* $\mathfrak{H}$ *durch ganze lineare homogene Substitutionen und bildet man zu jeder auf diese Weise erhaltenen irreduziblen linearen homogenen Substitutionsgruppe die zugehörige linear gebrochene Gruppe, so ist diese mit* $\mathfrak{H}$ *homomorph. Sieht man ähnliche Kollineationsgruppen als nicht verschieden an, so findet man auf die angegebene Art alle mit* $\mathfrak{H}$ *homomorphen irreduziblen Kollineationsgruppen. Der Grad jeder mit einer abstrakten endlichen Gruppe* $\mathfrak{H}$ *homomorphen irreduziblen Kollineationsgruppe ist ein Divisor der Ordnung von* $\mathfrak{H}$.

Das Problem, alle mit einer abstrakten endlichen Gruppe homomorphen Kollineationsgruppen zu bestimmen, ist von J. Schur, *Journ. f. Math.* **127**, 20 (1904), **132**, 85 (1907) durchgeführt worden. Hierin ist im besonderen die Bestimmung aller mit einer abstrakten Gruppe isomorphen Kollineationsgruppen niedrigsten Grades enthalten (Kleinsches Normalproblem).

Bedenkt man, daß bei jeder Permutation die Summe der Variablen $x_1 + x_2 + \cdots + x_n$ ungeändert bleibt und geht von der sich infolgedessen ergebenden Gruppe linearer homogener Substitutionen in $n - 1$ Variablen zu der zugehörigen Kollineationsgruppe in $n - 2$ Variablen über, so folgt, daß jede Permutationsgruppe n^{ten} Grades mit einer Kollineationsgruppe $n - 1^{\text{ten}}$ Grades, also einer solchen des Raumes R_{n-2} homomorph ist. Für die symmetrischen und alternierenden Permutationsgruppen gilt das Theorem (Wiman, *Math. Ann.* **52**, 243 (1899)):

Die symmetrische Gruppe $\mathfrak{S}_{n!}$ *und die alternierende Gruppe* $\mathfrak{A}_{\frac{n!}{2}}$ *sind mit Kollineationsgruppen* $n - 1^{ten}$ *Grades holoedrisch isomorph, nur für die* $\mathfrak{A}_{\frac{4!}{2}}$, *die* $\mathfrak{S}_{4!}$, *die* $\mathfrak{A}_{\frac{5!}{2}}$, *die* $\mathfrak{A}_{\frac{6!}{2}}$, *die* $\mathfrak{S}_{6!}$

und die $\mathfrak{A}_{\frac{7!}{2}}$ *existieren holoedrisch isomorphe Kollineationsgruppen niedrigeren Grades. Die* $\mathfrak{A}_{\frac{4!}{2}}$ *ist mit der Tetraedergruppe, die* $\mathfrak{S}_{4!}$ *mit der Oktaedergruppe und die* $\mathfrak{A}_{\frac{5!}{2}}$ *mit der Ikosaedergruppe des* R_1 (vgl. unten), *die* $\mathfrak{A}_{\frac{6!}{2}}$ *mit der Valentinergruppe des* R_2 (S. 242), *die* $\mathfrak{S}_{6!}$ *und* $\mathfrak{A}_{\frac{7!}{2}}$ *mit Kollineationsgruppen des* R_3 *holoedrisch isomorph.* Daß die $\mathfrak{S}_{6!}$ und $\mathfrak{A}_{\frac{7!}{2}}$ mit Kollineationsgruppen unseres R_3 holoedrisch isomorph sind, vgl. bei Klein (*Math. Ann.* **28**, 499 (1887)). Die Aufzählung der besonderen Kollineationsgruppen des R_2 und R_3, die mit symmetrischen und alternierenden Permutationsgruppen holoedrisch isomorph sind, findet man bei H. Maschke, *Math. Ann.* **51**, 253 (1899).

Betrachtet man ähnliche Kollineationsgruppen als nicht verschieden, so gibt es für $n > 7$ *im* R_{n-2} *nur eine einzige mit* $\mathfrak{S}_{n!}$ *bezw.* $\mathfrak{A}_{\frac{n!}{2}}$ *holoedrisch isomorphe Kollineationsgruppe; eine Ausnahme bildet nur der Fall* $n = 9$, *bei dem im* R_7 *zwei mit der alternierenden Gruppe von 9 Buchstaben isomorphe Kollineationsgruppen existieren.* (Wiman a. a. O.)

Sieht man ähnliche Kollineationsgruppen als nicht verschieden an, so existieren nach dem Jordanschen Satz (vgl. S. 227) *für einen gegebenen Grad n nur eine endliche Anzahl endlicher Kollineationsgruppen von wesentlich verschiedenem Typus.*

Es gibt fünf verschiedene Typen endlicher binärer Kollineationsgruppen, d. h. solcher des R_1.

1. Die *zyklische Gruppe* $\mathfrak{C}_g$. Sie hat als Kollineationsgruppe die Ordnung g und geht aus einer linearen homogenen Substitutionsgruppe der Determinante $+1$ hervor, die durch die lineare homogene Substitution S_1 mit der Matrix:

$$\begin{Vmatrix} e^{\frac{\pi i}{g}} & 0 \\ 0 & e^{-\frac{\pi i}{g}} \end{Vmatrix}, \quad e^{2\pi i} = 1$$

erzeugt wird.

2. Die *Diedergruppe* $\mathfrak{D}_{2g}$. Sie hat als Kollineationsgruppe die Ordnung $2g$ und geht aus einer linearen homogenen Sub-

stitutionsgruppe der Determinante $+1$ hervor, die durch zwei lineare homogene Substitutionen

$$S_1 = \begin{Vmatrix} e^{\frac{\pi i}{g}} & 0 \\ 0 & e^{-\frac{\pi i}{g}} \end{Vmatrix}, \quad S_2 = \begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix}$$

erzeugt wird.

3. Die *Tetraedergruppe* $\mathfrak{T}_{12}$. Sie hat als Kollineationsgruppe die Ordnung 12 und geht aus einer linearen homogenen Substitutionsgruppe der Determinante $+1$ hervor, die durch drei lineare homogene Substitutionen:

$$S_1 = \begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix}, \quad S_2 = \begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix}, \quad S_3 = \begin{Vmatrix} \frac{1-i}{2} & \frac{1-i}{2} \\ -\frac{1+i}{2} & \frac{1+i}{2} \end{Vmatrix}$$

erzeugt wird.

4. Die *Oktaedergruppe* $\mathfrak{O}_{24}$. Sie hat als Kollineationsgruppe die Ordnung 24 und geht aus einer linearen homogenen Substitutionsgruppe der Determinante $+1$ hervor, die durch die zwei linearen homogenen Substitutionen:

$$S_1 = \begin{Vmatrix} \sqrt{i} & 0 \\ 0 & \frac{1}{\sqrt{i}} \end{Vmatrix}, \quad S_2 = \begin{Vmatrix} \frac{1}{\sqrt{2i}} & \frac{1}{\sqrt{2i}} \\ \frac{1}{i\sqrt{2i}} & -\frac{1}{i\sqrt{2i}} \end{Vmatrix}$$

erzeugt wird.

5. Die *Ikosaedergruppe* $\mathfrak{J}_{60}$. Sie hat als Kollineationsgruppe die Ordnung 60 und geht aus einer linearen homogenen Substitutionsgruppe der Determinante $+1$ hervor, die durch die zwei linearen homogenen Substitutionen:

$$S_1 = \begin{Vmatrix} -\varepsilon^3 & 0 \\ 0 & -\varepsilon^2 \end{Vmatrix}, \quad S_2 = \begin{Vmatrix} \frac{1}{\varepsilon - \varepsilon^{-1}} & \frac{1}{\varepsilon^2 - \varepsilon^{-2}} \\ \frac{1}{\varepsilon^2 - \varepsilon^{-2}} & \frac{-1}{\varepsilon - \varepsilon^{-1}} \end{Vmatrix}$$

erzeugt wird; ε ist eine primitive fünfte Einheitswurzel.

Faßt man die obigen fünf Gruppen als Gruppen linearer homogener Substitutionen auf, so enthalten sie sämtlich die Ähnlichkeitssubstitution $\begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix}$ und haben daher doppelt so hohe Ordnungen als die Kollineationsgruppen $\mathfrak{C}_g$, $\mathfrak{D}_{2g}$, $\mathfrak{T}_{12}$, $\mathfrak{O}_{24}$ und $\mathfrak{J}_{60}$. *Nur für die endlichen Gruppen $\mathfrak{C}_g$ bei beliebigem g*

und die $\mathfrak{D}_{2g}$ *bei ungeradem* g *existieren holoedrisch isomorphe lineare homogene Substitutionsgruppen in zwei Variablen.*

Für $g = 2$ wird die aus den Kollineationen

$$\xi = \xi', \quad \xi = -\xi', \quad \xi = \frac{1}{\xi'}, \quad \xi = -\frac{1}{\xi'}$$

bestehende Diedergruppe $\mathfrak{D}_4$ als *Vierergruppe* bezeichnet.

Für $g = 3$ ist die Diedergruppe $\mathfrak{D}_6$ ähnlich mit der *anharmonischen Gruppe.* Diese liefert in der projektiven Geometrie die 6 zusammengehörigen Werte

$$\xi = \xi', \; \xi = \frac{1}{\xi'}, \; \xi = 1 - \xi', \; \xi = \frac{1}{1 - \xi'}, \; \xi = \frac{\xi' - 1}{\xi'}, \; \xi = \frac{\xi'}{\xi' - 1}$$

für das anharmonische Doppelverhältnis von vier Punkten einer Geraden und ferner die 6 zusammengehörigen Werte des Legendreschen Moduls k^2 eines elliptischen Integrals erster Gattung.

$\mathfrak{T}_{12}$ *und* $\mathfrak{J}_{60}$ *sind mit den alternierenden Permutationsgruppen in 4 bezw. 5 Symbolen holoedrisch isomorph. Die* $\mathfrak{O}_{24}$ *ist mit der symmetrischen Permutationsgruppe in 4 Symbolen holoedrisch isomorph.*

Die Kollineationsgruppen $\mathfrak{D}_{2g}$, $\mathfrak{T}_{12}$, $\mathfrak{O}_{24}$ *und* $\mathfrak{J}_{60}$ *sind mit den endlichen Gruppen holoedrisch isomorph, welche die regulären Körper „Dieder, Tetraeder, Oktaeder und Ikosaeder" mit sich zur Deckung bringen* (vgl. S. 176); hierbei gilt das reguläre g-Eck, *Dieder* genannt, auch als regulärer Körper. Die endlichen Kollineationsgruppen des R_1 werden daher auch als *Polyedergruppen* bezeichnet.

Sämtliche Substitutionen A der linearen homogenen homomorphen endlichen Substitutionsgruppen der Determinante $+1$ des R_1, aus denen die endlichen Kollineationsgruppen hervorgehen, lassen sich in die Form bringen:

$$x_1 = (a + ib)x_1' + (ci + d)x_2',$$
$$x_2 = (ci - d)x_1' + (a - ib)x_2',$$

wobei $a^2 + b^2 + c^2 + d^2 = 1$, $i = \sqrt{-1}$ und a, b, c, d reelle Größen bedeuten; dies folgt aus der symbolischen Gleichung $\overline{A}' = A^{-1}$ (vgl. S. 134 letzte Zeile), die besagt, daß alle endlichen Gruppen linearer homogener Substitutionen in zwei Variablen so transformierbar sind, daß sie die Hermitesche Form $x_1\overline{x}_1 + x_2\overline{x}_2$ in sich überführen. Die entsprechenden Kollineationen $\xi = \dfrac{(a + ib)\xi' + (ci + d)}{(ci - d)\xi' + (a - ib)}$ stellen die sämtlichen

Drehungen einer Kugel um ihren Durchmesser dar, wenn man die Kugel nach Riemann als Trägerin der komplexen Variablen ξ interpretiert (Cayley, *Math. Ann.* **16**, 260 (1880), Klein, *Ikosaeder*, S. 34).

Ein *volles Invariantensystem* für die oben angegebene lineare homogene Substitutionsgruppe, aus der die Diedergruppe $\mathfrak{D}_{2g}$ hervorgeht, bilden die drei Formen:

$$F_1 = x_1 x_2, \; F_2 = x_1^g + x_2^g, \; F_3 = x_1^g - x_2^g.$$

Sie sind sämtlich relative Invarianten der Gruppe. Zwischen ihnen besteht die Relation $4 F_1^{2g} = F_2^2 - F_3^2$.

Ein volles Invariantensystem für die lineare homogene Substitutionsgruppe, aus der die Tetraedergruppe $\mathfrak{T}_{12}$ hervorgeht, bilden die Formen:

$$f_4 = x_1^4 + 2\sqrt{-3}\, x_1^2 x_2^2 + x_2^4,$$
$$f_4' = x_1^4 - 2\sqrt{-3}\, x_1^2 x_2^2 + x_2^4,$$
$$f_6 = x_1 x_2 (x_1^4 - x_2^4).$$

Zwischen ihnen besteht die Relation:

$$12\sqrt{-3}\, f_6^2 = f_4^3 - f_4'^3.$$

f_6 ist eine absolute Invariante der Gruppe, f_4 und f_4' sind relative Invarianten vom Index 3. Ein volles System absoluter Invarianten bilden f_6, $H_8 = f_4 \cdot f_4'$, f_4^3.

Ein volles Invariantensystem für die lineare homogene Substitutionsgruppe, aus der die Oktaedergruppe $\mathfrak{O}_{24}$ hervorgeht, bilden die drei Formen:

$$f_6 = x_1 x_2 (x_1^4 - x_2^4),$$
$$H_8 = f_4 f_4' = x_1^8 + 14 x_1^4 x_2^4 + x_2^8,$$
$$K = \tfrac{1}{2}(f_4^3 + f_4'^3) = x_1^{12} - 33 x_1^8 x_2^4 - 33 x_1^4 x_2^8 + x_2^{12}.$$

Zwischen ihnen besteht die Relation:

$$108 f_6^4 = H_8^3 - K^2.$$

Die Form H_8 ist eine absolute Invariante, f_6 und K sind relative Invarianten vom Index 2. Ein volles System absoluter Invarianten bilden die drei Formen H_8, f_6^2 und $f_6 \cdot K$.

Ein volles Invariantensystem für die lineare homogene Substitutionsgruppe, aus der die Ikosaedergruppe hervorgeht, bilden die drei Formen:

$$f_{12} = x_1 x_2 (x_1^{10} + 11 x_1^5 x_2^5 - x_2^{10}),$$
$$H_{20} = -(x_1^{20} + x_2^{20}) + 228(x_1^{15} x_2^5 - x_2^{15} x_1^5) - 494 x_1^{10} x_2^{10},$$
$$T = x_1^{30} + x_2^{30} + 522(x_1^{25} x_2^5 - x_1^5 x_2^{25}) - 10005(x_1^{20} x_2^{10} + x_2^{20} x_1^{10}).$$

Zwischen ihnen besteht die Relation:

$$T^2 + H_{20}^3 = 1728 f_{12}^5.$$

Die drei Formen f_{12}, H_{20} und T sind absolute Invarianten; für die Ikosaedergruppe existieren keine relativen Invarianten.

Die Formen f_4, f_4', f_6 und f_{12} und die aus ihnen durch lineare homogene Transformation hervorgehenden sind die einzigen binären Formen ohne vielfache Faktoren, deren vierte Überschiebung $(f, f)^4$ verschwindet. (Wedekind, *Habilit.-Schr.*, Karlsruhe (1876), Brioschi, *Ann. di mat.* (2) **8**, 24 (1877), Gordan, *Vorlesungen über Invariantentheorie* **2**, 204.)

H_8 ist die Hessesche Determinante von f_6, H_{20} die von f_{12}, f_4' die von f_4 und f_4 die von f_4', f_6 ist die Funktionaldeterminante von f_4 und f_4', K von f_6 und H_8, T von H_{20} und f_{12}.

Die Form f_4 entspricht den Ecken des Tetraeders, f_4' denjenigen des Gegentetraeders, f_6 den Kantenhalbierungspunkten, die ein Oktaeder bilden. Ebenso liegt es bei den Invarianten des Oktaeders und des Ikosaeders; f_6 entspricht den Oktaederecken, H_8 dem Polarwürfel, K den 12 Kantenhalbierungspunkten, f_{12} entspricht den Ikosaederecken, H_{20} den Ecken des reziproken Pentagondodekaeders und T den Kantenhalbierungspunkten. Die Hesseschen Determinanten entsprechen also den Mitten der Seitenflächen der betrachteten Polyeder, die Funktionaldeterminanten den Mittelpunkten der Kanten der Polyeder. Setzt man $\frac{x_1}{x_2} = \vartheta$ und bildet sich $\frac{f_4^3}{f_4'^3} = Z$, $\frac{H_8^3}{108 f_6^4} = Z$, $\frac{H_{20}^3}{1728 f_{12}^5} = Z$, so ist Z Funktion von ϑ. Die drei auf diese Weise definierten Gleichungen $f(\vartheta) = Z$ vom Grade 12, 24 und 60 heißen nach Klein die *Tetraeder-*, *Oktaeder-* und *Ikosaedergleichung.* Die letztere Gleichung lautet ausführlich:

$$(-\vartheta^{20} - 1 + 228\vartheta^{15} - 228\vartheta^5 - 494\vartheta^{10})^3 - 1728\vartheta^5 Z(\vartheta^{10} + 11\vartheta^5 - 1)^5 = 0.$$

ϑ als Funktion von Z aufgefaßt, heißt die Irrationalität des Tetraeders bezw. des Oktaeders und Ikosaeders.

Wir vermerken noch die *Untergruppen der Ikosaedergruppe.* Sie sind zyklische Gruppen: fünfzehn $\mathfrak{C}_2$, zehn $\mathfrak{C}_3$, sechs $\mathfrak{C}_5$, Diedergruppen: fünf $\mathfrak{D}_4$, zehn $\mathfrak{D}_6$, sechs $\mathfrak{D}_{10}$ und 5 Tetraedergruppen $\mathfrak{T}_{12}$. Gruppen gleicher Ordnung sind in bezug auf die Ikosaedergruppe konjugiert.

Die endlichen Kollineationsgruppen des R_1 sind zuerst von F. Klein, *Math. Ann.* **9**, 183 (1876), und zwar auf geometrischem Wege durch Betrachtung der Drehungen einer Kugel um ihren Durchmesser und der der Kugel einbeschriebenen Polyeder bestimmt worden. Die erste algebraische Herleitung der endlichen Kollineationsgruppen des R_1 gab Gordan, *Math. Ann.* **12**, 23 (1877). Auf die invarianten binären Formen in unhomogener Gestalt war bereits H. A. Schwarz, *Journ. f. Math.* **75**, 323 (1873) bei der Bestimmung der Fälle gelangt, in denen die Gaußsche Differentialgleichung der hypergeometrischen Funktion durch algebraische Funktionen befriedigt wird. Vgl. die systematischen Darstellungen bei Klein, *Ikosaeder*, H. Weber, *Algebra* **2**, 269, Bianchi, *Teoria dei gruppi,* S. 99, Vivanti, *Elementi della teoria delle funzioni poliedriche e modulari,* Milano 1906.

Die Aufzählung der endlichen ternären Kollineationsgruppen, d. h. derjenigen des R_2 hat zuerst C. Jordan (*Journ. f. Math.* **84**, 89 (1878)) unternommen; hierbei entgingen ihm eine von F. Klein (*Math. Ann.* **14**, 428 (1879)) entdeckte Gruppe der Ordnung 168 und eine von Valentiner (*Videnskabernes Selskabs Skrifter,* 6. Raekke (1889), Kopenhagen) gefundene Gruppe der Ordnung 360. Eine erneute Bestimmung der endlichen ternären Kollineationsgruppen gab Blichfeldt, *Math. Ann.* **63**, 552 (1907).

Abgesehen von reduziblen Kollineationsgruppen und solchen, bei denen sich die Variablen der zugehörigen homogenen linearen Substitutionsgruppen bis auf konstante Faktoren nur untereinander permutieren (*Monomialgruppen,* Maschke, *Am. J. math.* **17**, 168 (1895)), *gibt es, wenn ähnliche Kollineationsgruppen als nicht verschieden gelten, sechs verschiedene Arten endlicher ternärer Kollineationsgruppen, d. h. solcher der Ebene.*

1. Die *Hessesche Gruppe*, die als Kollineationsgruppe die *Ordnung 216* hat und aus keiner niedrigeren ternären linearen homogenen Substitutionsgruppe als einer solchen der Ordnung 648 herleitbar ist. Der Name der Gruppe stammt daher, weil sie mit der Hesseschen Konfiguration zusammenhängt, die sich bei der Betrachtung des syzygetischen Büschels $kf + \lambda\Delta = 0$ ergibt, der von einer Kurve dritter Ordnung $f = 0$ und ihrer

Hesseschen Kurve Δ gebildet wird. Eine Invariante der Gruppe ist die Form, welche die vier Wendepunktdreiecke des Büschels bestimmt. Das volle Invariantensystem, das aus fünf Formen besteht, findet man bei Maschke, *Math. Ann.* **33**, 326 (1889).

2. *Eine invariante Untergruppe der Hesseschen Gruppe von der Ordnung 72* bezw. 216 bei homogener Schreibweise.

3. *Eine Untergruppe der Hesseschen Gruppe von der Ordnung 36* bezw. 108 bei homogener Schreibweise. Die Hessesche Gruppe enthält drei solcher Gruppen; sie haben eine in der Hesseschen Gruppe der Ordnung 216 invariante Untergruppe der Ordnung 18 gemein. Die Hessesche Gruppe ist daher mit der Tetraedergruppe $\mathfrak{T}_{12}$ homomorph; nach ihr transformieren sich die Formen f und Δ.

4. Die *ternäre Ikosaedergruppe,* die als Kollineationsgruppe die Ordnung 60 hat und aus einer linearen homogenen ternären Substitutionsgruppe derselben Ordnung 60 hervorgeht.

5. Die *Kleinsche Gruppe,* die als Kollineationsgruppe die Ordnung 168 hat und aus einer linearen homogenen ternären Substitutionsgruppe derselben Ordnung 168 hervorgeht. Die Gruppe ist *einfach* und, da es nur eine einfache abstrakte Gruppe der Ordnung 168 gibt, holoedrisch isomorph mit der Modulargruppe für die Primzahl $p = 7$ (vgl. S. 201). Die Invariante niedrigsten Grades der homogenen Gruppe ist die ternäre Form

$$x_1{}^3 x_3 + x_2{}^3 x_1 + x_3{}^3 x_2 .$$

Die Gruppe besitzt nur absolute Invarianten. Das volle Invariantensystem besteht aus vier Formen. Die Gruppe ist gefunden von Klein, *Math. Ann.* **14**, 428 (1879), vgl. ferner Klein, *Math. Ann.* **15**, 265 (1879), Gordan, ebenda **17**, 217, 359 (1880), **20**, 515 (1882), **25**, 459 (1885). Systematische Darstellungen bei Klein-Fricke, *Modulfunktionen* **1**, 692 u. H. Weber, *Algebra* **2**, 497.

6. Die *Valentinersche Gruppe,* die als Kollineationsgruppe die Ordnung 360 hat und aus keiner niedrigeren homogenen linearen ternären Gruppe als einer solchen der Ordnung 1080 hervorgeht. *Die Valentinersche Gruppe ist mit der alternierenden Permutationsgruppe in sechs Symbolen holoedrisch isomorph.* Sie enthält zwei Systeme von je sechs konjugierten Ikosaedergruppen und zwei Systeme von je 15 konjugierten Oktaedergruppen. Die Invariante niedrigsten Grades der homogenen Gruppe ist von der Form:

$$10 x_1{}^3 x_2{}^3 + 9 x_3 (x_1{}^5 + x_2{}^5) - 45 x_1{}^2 x_2{}^2 x_3{}^2 - 135 x_1 x_2 x_3{}^4 + 27 x_3{}^6 .$$

Das volle Invariantensystem der Gruppe besteht aus vier Formen und ist zuerst von Wiman, *Math. Ann.* **47**, 531 (1896) aufgestellt worden. Vgl. ferner Gerbaldi, *Rend. Circolo di Palermo,* **12**, 23 (1898), **13**, 161 (1899), **14**, 66 (1900), **16**, 129 (1902), *Math. Ann.* **50**, 473 (1898), Fricke, *Gött. Nachr.* (1896), 199, *Math. Ver.* **5**, 55 (1896), L. Lachtin, *Math. Ann.* **51**, 463 (1899), Gordan, *Math. Ann.* **61**, 453 (1905).

Die vollständige Aufzählung der verschiedenen endlichen quaternären Kollineationsgruppen, d. h. derjenigen unseres R_3, stammt von Blichfeldt, *Math. Ann.* **60**, 204 (1905), *Trans. Am. M. S.* **6**, 230 (1905). Vgl. ferner Autonne, *Journ. de math.* (5) **7**, 351 (1901) u. Bagnera, *Rend. Circolo di Palermo* **19**, 1 (1905). Im R_3 gibt es allein 25 nicht ähnliche Kollineationsgruppen, die mit symmetrischen und alternierenden Permutationsgruppen holoedrisch isomorph sind (Maschke, *Math. Ann.* **51**, 298 (1899)), hierunter je eine mit $\mathfrak{S}_{6!}$ und $\mathfrak{A}_{\frac{7!}{2}}$ isomorphe Gruppe. Besonders bemerkenswert sind unter den quaternären endlichen Kollineationsgruppen:

1. eine solche der Ordnung 11520, die aus einer homogenen quaternären linearen Substitutionsgruppe von viermal so hoher Ordnung hervorgeht,

2. eine solche der Ordnung 25920, die sich aus einer homogenen quaternären linearen Substitutionsgruppe von doppelt so hoher Ordnung ergibt.

Nach der Kollineationsgruppe der Ordnung 11520, die F. Klein (*Math. Ann.* **2**, 198 (1870), **4**, 356 (1871)) durch liniengeometrische Betrachtungen gefunden hat, transformieren sich die Verhältnisse der bei den hyperelliptischen Funktionen des Geschlechtes $p = 2$ auftretenden sogenannten Borchardtschen Moduln. Die $\mathfrak{G}_{11520}$ ist holoedrisch isomorph mit der Galoisschen Gruppe der Gleichung 16ten Grades, welche die 16 Knotenpunkte einer Kummerschen Fläche bestimmt (Jordan, *Traité*, 313) und homomorph mit der symmetrischen Gruppe $\mathfrak{S}_{6!}$. Ein volles Invariantensystem der homogenen Gruppe ist von Maschke, *Math. Ann.* **30**, 496 (1887) aufgestellt worden. Weitere Literatur: Reichardt, *Math. Ann.* **28**, 84 (1887), *Nova Acta Leop.* **50**, 375 (1887), Heß, ebenda **55**, 100 (1891).

Die Kollineationsgruppe $\mathfrak{G}_{25920}$ ist *einfach.* Sie ist holoedrisch isomorph mit einer invarianten Untergruppe des Index 2 der Galoisschen Gruppe $\mathfrak{G}'_{51840}$ der Ordnung 51840 der Gleichung für die Bestimmung der 27 Geraden einer allgemeinen Fläche

dritter Ordnung; von dieser $\mathfrak{G}'_{51840}$ hängt auch die Dreiteilung der hyperelliptischen Funktionen ab. (C. Jordan, *Traité*, 316 u. 365, F. Klein, *Journ. de math.* (4) **4**, 169 (1888), H. Burkhardt, *Math. Ann.* **38**, 161 (1891), **41**, 313 (1893).) Das volle Invariantensystem der homogenen $\mathfrak{G}_{51840}$[1]), die mit der Kollineationsgruppe $\mathfrak{G}_{25940}$ homomorph ist, bei H. Maschke, *Math. Ann.* **33**, 317 (1889). Eine gruppentheoretische Untersuchung dieser vielfach behandelten Gruppe mit Literaturangaben bei Dickson, *Trans. Am. M. S.* **5**, 126 (1904), *Proc. Lond. M. S.* (2) **1**, 283 (1904), vgl. auch Dickson, *Linear groups*, S. 303, W. Burnside, *Proc. Royal Soc.* A **77**, 182 (1906). Vgl. auch S. 249.

Erwähnt sei noch, daß nach den Untersuchungen von J. Schur, *Journ. f. Math.* **132**, 135 (1907) über die Darstellungen der verallgemeinerten Modulargruppe als Kollineationsgruppen die einfache Gruppe der Ordnung 504 sich als Kollineationsgruppe in sechs und nicht weniger Variablen darstellen läßt, während die voraufgehenden einfachen Gruppen der Ordnungen 60 und 168 als Kollineationsgruppen in einer bezw. zwei Variablen darstellbar sind. Es gilt folgender allgemeiner Satz: Ist $p^m > 3$, aber von 9 verschieden, so gibt es, wenn p eine ungerade Primzahl ist, im ganzen $\frac{p^m+3}{2}$ verschiedene irreduzible Gruppen ganzer linearer homogener Substitutionen, die *mit der verallgemeinerten endlichen Modulargruppe* (vgl. S. 215) *der Ordnung* $\frac{p^m(p^{2m}-1)}{2}$ *isomorph sind,* und zwar eine des Grades p^m, $\frac{p^m-4-\varepsilon}{4}$ des Grades p^m+1, $\frac{p^m-2+\varepsilon}{4}$ des Grades p^m-1 und zwei des Grades $\frac{p^m+\varepsilon}{2}$. Ebenso gibt es für $p^m > 3$, aber $\neq 9$, $\frac{p^m+3}{2}$ verschiedene irreduzible Kollineationsgruppen, die mit der verallgemeinerten Modulargruppe isomorph sind und sich nicht als Gruppen von $\frac{p^m(p^{2m}-1)}{2}$ ganzen linearen homogenen Substitutionen schreiben lassen. Unter diesen Gruppen haben $\frac{p^m-2+\varepsilon}{4}$ den Grad p^m+1, $\frac{p^m-\varepsilon}{4}$ den Grad p^m-1 und zwei den Grad $\frac{p^m-\varepsilon}{2}$; hierbei ist $\varepsilon = (-1)^{\frac{p^m-1}{2}}$. Es gibt 2^m verschiedene irreduzible Kollineationsgruppen, die mit

---

1) $\mathfrak{G}_{51840}$ und $\mathfrak{G}'_{51840}$ sind natürlich nicht isomorph; die erste Gruppe hat eine invariante Untergruppe zweiter Ordnung, die zweite eine invariante Untergruppe $\mathfrak{G}_{25920}$.

der *verallgemeinerten endlichen Modulargruppe der Ordnung* $2^m(2^{2m}-1)$ *des* $GF[2^m]$ *für* $2^m > 4$ *isomorph* sind, und zwar hat man eine Gruppe des Grades 2^m, ferner $2^{m-1}-1$ des Grades 2^m+1 und 2^{m-1} des Grades 2^m-1. Alle diese Gruppen lassen sich auch als ganze lineare homogene Substitutionsgruppen derselben Ordnung $2^m(2^{2m}-1)$ darstellen. (J. Schur, a. a. O., 133 u. 134.) Die mit der gewöhnlichen Modulargruppe ($m=1$) isomorphen Kollineationsgruppen des Grades $\frac{p-1}{2}$ bezw. $\frac{p+1}{2}$, d. h. des $R_{\frac{p-3}{2}}$ bezw. $R_{\frac{p-1}{2}}$, hat F. Klein, *Math. Ann.* **15**, 275 (1879) aus der Transformationstheorie der elliptischen Funktionen gefunden.

§ 12. Lineare Gruppen mit Koeffizienten aus einem Körper. Kongruenzgruppen.

Die Gesamtheit aller Kollineationen A_1:

$$\xi_i = \frac{a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in}\xi_n' + a_{in+1}}{a_{n1}\xi_1' + a_{n2}\xi_2' + \cdots + a_{nn}\xi_n' + a_{nn+1}} \qquad (i=1,2,\ldots,n)$$

gleichen Grades $n+1$ mit nicht verschwindenden Determinanten $|a_{ik}|$ $(i,k=1,2,\ldots,n+1)$, deren Koeffizienten sämtlich ausnahmslos einem Körper Ω angehören, bildet eine Gruppe; sie heißt die *allgemeine projektive oder linear gebrochene Gruppe in n Variablen* oder die *allgemeinste Kollineationsgruppe* $(n+1)^{ten}$ *Grades mit Koeffizienten aus* Ω. Ist Ω ein endlicher Körper (vgl. S. 177), so ist die Gruppe selbst *endlich*; man spricht von der *allgemeinen projektiven oder linear gebrochenen* oder *allgemeinsten Kollineationsgruppe mit Koeffizienten aus dem* $GF[p^m]$ (Galoissches Feld der Ordnung p^m) oder kürzer von einer *allgemeinen linear gebrochenen Kongruenzgruppe.*

Die Gesamtheit aller Substitutionen

$$\xi_i = a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in}\xi_n' + a_{in+1} \qquad (i=1,2,\ldots,n)$$

gleichen Grades mit nicht verschwindenden Determinanten $|a_{ik}|$ $(i,k=1,2,\ldots,n)$, deren Koeffizienten ausnahmslos einem Körper Ω angehören, bildet die *allgemeine lineare unhomogene Gruppe* oder die *allgemeine volle lineare Gruppe mit Koeffizienten aus* Ω. Sie hat die *kommutative Gruppe*: $\xi_i = \xi_i' + a_{in+1}$ $(i=1,2,\ldots,n)$ zur *invarianten Untergruppe*. Die letztere Gruppe wird auch, wenn Ω das $GF[p^m]$ ist, als *arithmetische Gruppe* bezeichnet.

In der allgemeinen linearen unhomogenen Gruppe mit Koeffizienten aus Ω ist die *allgemeine lineare homogene Gruppe*

mit Koeffizienten aus Ω als Untergruppe enthalten. Sie besteht aus der Gesamtheit aller Substitutionen:

$$\xi_i = a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in}\xi_n' \qquad (i = 1, 2, \ldots, n)$$

mit nicht verschwindenden Determinanten $|a_{ik}|$ $(i, k = 1, 2, \ldots, n)$ und Koeffizienten aus Ω.

Ist Ω *das* $GF[p^m]$, *so hat die allgemeine lineare homogene Kongruenzgruppe* n^{ten} *Grades*[1]) *die Ordnung*

$$h = (p^{mn} - 1)(p^{mn} - p^m) \cdot (p^{mn} - p^{2m}) \cdots (p^{mn} - p^{m(n-1)})$$

und die volle Gruppe die Ordnung $h \cdot p^{mn}$.

Läßt man in dem Symbol $l_{\xi_1'\xi_2'\ldots\xi_n'}$ die n Indices die p^m Marken des $GF[p^m]$ durchlaufen und ersetzt ξ_i' durch

$$\xi_i = a_{i1}\xi_1' + a_{i2}\xi_1' + \cdots + a_{in}\xi_n' + a_{in+1} \quad (i = 1, 2, \ldots, n),$$

wobei die Koeffizienten a_{ik} alle Zahlen des $GF[p^m]$ mit nicht verschwindenden Determinanten $|a_{ik}|$ $(i, k = 1, 2, \ldots, n)$ durchlaufen, so entspricht jeder linearen unhomogenen Substitution eine Permutation unter den p^{mn} Größen $l_{\xi_1'\xi_2'\ldots\xi_n'}$. Die aus diesen Permutationen bestehende Gruppe ist mit der linearen unhomogenen Substitutionsgruppe mit Koeffizienten aus dem $GF[p^m]$ holoedrisch isomorph. Anstatt ein Symbol l mit n Indices zu verwenden, kann man auch ein Symbol l_ζ mit nur einem Index ζ verwenden, den man die p^{nm} Marken des $GF[p^{mn}]$ durchlaufen läßt. Ersetzt man ζ durch eine geeignet gewählte ganze rationale Funktion $\psi(\zeta)$ von ζ mit Koeffizienten aus dem $GF[p^{mn}]$, so stellt $\begin{pmatrix} l_\zeta \\ l_{\psi(\zeta)} \end{pmatrix}$, wenn ζ die Zahlen des $GF[p^{mn}]$ durchläuft, eine Permutation unter den p^{mn} Größen l_ζ dar. Auch eine aus derartigen Permutationen bestehende Permutationsgruppe des $p^{mn\,\text{ten}}$ Grades läßt sich der linearen unhomogenen Substitutionsgruppe mit Koeffizienten aus dem $GF[p^m]$ holoedrisch isomorph zuordnen. (Betti, *Ann. di scienze mat. e fis.* **3** (1852), **6** (1855), *Opere mat.*, Milano 1903, **1**, 48 u. 117, Mathieu, *Journ. de math.* (2) **6**, 301 (1861), Dickson, *Linear groups*, S. 64 u. 75.)

Die sich für $m = 1$ ergebende Permutationsgruppe tritt bereits in folgendem berühmtem Satze von Galois (*Œuvres*, p. 27) auf:

---

1) Unter dem Grad einer linearen homogenen Gruppe versteht man die Variablenzahl. Eine Kongruenzgruppe erhält man auch, wenn man alle linearen homogenen Substitutionen gleichen Grades mit ganzzahligen Koeffizienten mod s betrachtet, deren Determinanten zu s relativ prim sind, wobei s eine beliebig gewählte, ganze positive Zahl bedeutet. (C. Jordan, *Traité*, S. 92.)

Jede primitive Permutationsgruppe des Grades p^n (p Primzahl) kann nur dann auflösbar sein, wenn sie eine Untergruppe der Permutationsgruppe $p^{n \text{ten}}$ Grades der Ordnung

$$(p^n - 1)(p^n - p)(p^n - p^2)\ldots(p^n - p^{n-1})p^n$$

ist, die mit der allgemeinen vollen linearen Kongruenzgruppe mit Koeffizienten mod p in n Variablen holoedrisch isomorph ist. Für $n = 1$ ist die Gruppe immer auflösbar, vgl. S. 213. Für $n > 1$ ist die Gruppe der Ordnung $(p^n - 1)(p^n - p)(p^n - p^2)\ldots(p^n - p^{n-1})p^n$ nicht stets auflösbar; mit der Bestimmung ihrer sämtlichen auflösbaren Untergruppen beschäftigt sich C. Jordan, *Traité*, S. 398ff. Von Lehrbüchern vgl. H. Weber, *Algebra* **2**, 359. Für $p = 3$, $n = 2$ hat die Gruppe die Ordnung 432. Diese Gruppe ist eine auflösbare Gruppe und die Galoissche Gruppe der *Gleichung neunten Grades,* von der die Bestimmung der *9 Wendepunkte einer Kurve dritter Ordnung* abhängt (Hesse, *Journ. f. Math.* **34** (1847), *Ges. Werke*, 137; vgl. auch H. Weber, *Algebra* **2**, 410, Netto, *Algebra* **2**, 460).

Die Gesamtheit aller linear gebrochenen Substitutionen:

$$\xi_i = \frac{a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in}\xi_n' + a_{in+1}}{a_{n1}\xi_1' + a_{n2}\xi_2' + \cdots + a_{nn}\xi_n' + a_{nn+1}} \qquad (i = 1, 2, \ldots, n)$$

mit Koeffizienten aus einem Körper Ω, bei denen die Determinante $|a_{ik}|$ $(i, k = 1, 2 \ldots, n+1)$ den Wert $+1$ hat, heißt die *spezielle Kollineationsgruppe $n + 1^{\text{ten}}$ Grades* oder die *spezielle linear gebrochene Gruppe oder die spezielle projektive Gruppe mit Koeffizienten aus Ω.* Sie ist eine invariante Untergruppe der allgemeinen projektiven Gruppe mit Koeffizienten aus Ω.

Ist Ω das $GF[p^m]$, so ist die spezielle linear gebrochene Gruppe in n Variablen endlich und hat die Ordnung

$$\frac{1}{d}(p^{m(n+1)} - 1)p^{mn}(p^{mn} - 1)p^{m(n-1)}\ldots(p^{2m} - 1)p^m,$$

wobei d der größte gemeinsame Teiler von $n + 1$ und $p^m - 1$ ist. Ausgenommen in den zwei Fällen $(n + 1, p^m) = (2, 2)$ und $(2, 3)$ ist die endliche spezielle linear gebrochene Gruppe eine einfache Gruppe. Ist die Zahl n im besonderen gleich 1, so erhält man die verallgemeinerte Modulargruppe der Ordnung $(2^{2m} - 1) \cdot 2^m$ bezw. $\frac{(p^{2m} - 1)}{2} p^m$, falls $p > 2$. Für $n = 2$, $p = 2$, $m = 1$ hat die spezielle lineare gebrochene Gruppe in 2 Variablen die Ordnung 168. Als einfache Gruppe muß sie, da es nur eine einfache Gruppe der Ordnung 168 gibt, mit der Modulargruppe

für $p = 7$ holoedrisch isomorph sein. Über die spezielle linear gebrochene Gruppe für $n = 2$, p^m bei beliebigem m vgl. Dickson, *Linear groups,* S. 242.

Die Gesamtheit aller linearen homogenen Substitutionen

$$\xi_i = a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in}\xi_n' \qquad (i = 1, 2, \ldots, n)$$

mit Koeffizienten aus einem Körper Ω, bei denen die Determinante $|a_{ik}|$ den Wert $+1$ hat, heißt die *spezielle lineare homogene Gruppe mit Koeffizienten aus* Ω. Die Gruppe hat die aus den Ähnlichkeitstransformationen $\xi_i = \nu\xi_i'$ $(\nu^n = 1)$ gebildete Gruppe zur invarianten Untergruppe, wobei ν alle Größen aus Ω durchläuft.

Ist Ω ein *algebraischer Zahlkörper*, so bildet die Gesamtheit aller linearen homogenen Substitutionen der Determinante $+1$, deren Koeffizienten ausnahmslos *ganze algebraische Zahlen* des Körpers sind, eine Gruppe. Diese Gruppe wird von einer *endlichen Anzahl von Elementen erzeugt.* (Vgl. S. 193.) (A. Hurwitz, *Gött. Nachr.* (1895), 332.) Im besonderen wird also auch die Gruppe aller ganzzahligen linearen homogenen Substitutionen der Determinante $+1$ von einer endlichen Anzahl von Substitutionen erzeugt; für diesen speziellen Fall genügen sogar zwei erzeugende Substitutionen (Kronecker, *Monatsb. d. Berl. Akad.* (1866), *Ges. Werke* **1**, 159, Krazer, *Ann. di mat.* (2) **12**, 283 (1884), W. Burnside, *Messenger of mat.* **33**, 133 (1904)).

Als Untergruppe der speziellen linearen homogenen Gruppe sei für $n = 2r$ die *spezielle lineare Abelsche Gruppe* angeführt. (Die Bezeichnung hat mit kommutativer Gruppe (vgl. S. 174) nichts zu tun; die Gruppe stammt aus der Theorie der Abelschen Funktionen (Jordan, *Traité,* S. 171)). Die spezielle lineare Abelsche Gruppe besteht aus der Gesamtheit aller linearen homogenen Substitutionen:

$$\xi_i = a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in}\xi_n', \qquad (i = 1, 2, \ldots, 2r)$$

welche die alternierende bilineare Form:

$$\xi_1\eta_2 - \xi_2\eta_1 + \xi_3\eta_4 - \xi_4\eta_2 + \cdots + \xi_{2r-1}\eta_{2r} - \xi_{2r}\eta_{2r-1}$$

mit kogredienten Variablen ξ_i, η_i in sich überführen. *Ist* Ω *das* $GF[p^m]$, *so hat die sich aus der speziellen linearen Abelschen Gruppe ergebende Gruppe linear gebrochener Substitutionen die Ordnung*

$$\frac{1}{a}(p^{m(2r)} - 1) \cdot p^{m(2r-1)} \cdot (p^{m(2r-2)} - 1) p^{m(2r-3)} \ldots (p^{2m} - 1) p^m,$$

wobei $a = 1$ *oder* $= 2$, *je nachdem* $p = 2$ *oder* > 2 *ist. Außer für die drei Fälle* $p^m = 2$, $r = 1$ *und* $r = 2$, $p^m = 3$, $r = 1$ *ist die spezielle linear gebrochene Abelsche Gruppe einfach* (vgl. S. 202 erste Zeile). Die einfache Gruppe niedrigster Ordnung, die in diesem System enthalten ist, ist eine solche der Ordnung 25920, die $p^m = 3$, $r = 2$ entspricht und mit der einfachen Kollineationsgruppe des R_3 (vgl. S. 243) holoedrisch isomorph ist. $p^m = 2$, $r = 3$ ergibt die einfache Gruppe der Ordnung 1451520; sie ist holoedrisch isomorph mit der Galoisschen Gruppe der *Gleichung der 28 Doppeltangenten einer Kurve vierter Ordnung ohne Doppelpunkte.* Eine Untergruppe der Gruppe $\mathfrak{G}_{1451520}$ vom Index 28 ist holoedrisch isomorph mit der Galoisschen Gruppe $\mathfrak{G}'_{51840}$ (vgl. S. 244) der Gleichung für die 27 Geraden einer Fläche dritter Ordnung. (Jordan, *Traité,* S. 229 u. 330, H. Weber, *Algebra* **2**, 419.) Vgl. auch Dickson, *Trans. Am. M. S.* **3**, 38 u. 377 (1902), *Am. J. math.* **26**, 243 (1904).

Die Gesamtheit aller linearen homogenen Substitutionen

$$\xi_i = a_{i1}\xi_1' + a_{i2}\xi_2' + \cdots + a_{in}\xi_n' \qquad (i = 1, 2, \ldots, n),$$

mit Koeffizienten aus einem Körper Ω, die $\xi_1^2 + \xi_2^2 + \cdots + \xi_n^2$ in sich transformieren, bildet die *orthogonale Gruppe mit Koeffizienten aus* Ω. Ihre Behandlung für das $GF[p^m]$ bei Dickson, *Linear groups,* S. 156. Wegen weiterer Einzelheiten in bezug auf Kongruenzgruppen vgl. das zitierte Werk, sowie in Ergänzung für beliebige Körper: Dickson, *Trans. Am. M. S.* **2**, 363 (1901).

In Analogie mit dem in § 10 behandelten Problem der Darstellung einer abstrakten Gruppe als Gruppe linearer homogener Substitutionen kann man sich die Aufgabe stellen: Es ist eine endliche Gruppe $\mathfrak{G}$ gegeben. Man soll mit ihr homomorphe lineare homogene Substitutionsgruppen mit Koeffizienten aus einem $GF[p^m]$ konstruieren. Vgl. Dickson, *Trans. Am. M. S.* **8**, 389 (1907), *Bull. Am. M. S.* (2) **13**, 477 (1907).

Wir führen nur folgendes Theorem von Blichfeldt (*Trans. Am. M. S.* **8**, 30 (1907)) an:

Ist $\mathfrak{G}$ *eine irreduzible lineare homogene Substitutionsgruppe in n Variablen, so kann man stets unendlich viele derartige Primzahlen p finden, daß sich mittelst jeder von ihnen eine zu* $\mathfrak{G}$ *holoedrisch isomorphe irreduzible Gruppe* $\mathfrak{G}_1$ *linearer homogener Substitutionen in ebenfalls n Variablen bilden läßt, deren Koeffizienten ausschließlich ganze, mod p zu nehmende Zahlen sind.*